297-2621-301

Digital Switching Systems

UCS DMS-250

Software Optionality Control User's Manual

UCS17 Standard 10.03 July 2002

NORTEL NETWORKS™

Digital Switching Systems

UCS DMS-250

Software Optionality Control User's Manual

Publication number: 297-2621-301
Product release: UCS17
Document release: Standard 10.03
Date: July 2002

Contents

Publication history

July 2002

Standard release 10.03 for changes to software release UCS17 (CSP17), added to Standard release 09.02 for software release UCS14 (CSP14).

April 2002

Preliminary release 10.02 for software release UCS17. Change page release combined with UCS14 Standard release.

March 2002

Preliminary change page release 10.01 for UCS17 that included change to UTRS0201 through 59033229 - UCS16: Jurisdiction Option Enhancement.

November 2000

Standard release 09.02 for software release UCS14 (CSP14). This document was revised to include SOC OAM00010.

May 2000

Standard release 08.02 for software release UCS13 (CSP13).

March 2000

Preliminary release 08.01 for software release UCS13 (CSP13). This document was revised to add SOC UBFR0006.

January 1999

Standard release 07.01 for software release UCS12 (CSP12). This document was revised to add SOC NXXR0003 (PSD07023). Revised EADAS SOC names.

May 1999

Standard release 06.02 for software release UCS11 (CSP11). This document was revised for SOC name changes.

March 1999

Preliminary release 06.01 for software release UCS11 (CSP11).

About this document

When to use this document

This document describes software optionality control (SOC) and how to use it.

How to check the version and issue of this document

The version and issue of the document are indicated by numbers, for example, 01.01.

The first two digits indicate the version. The version number increases each time the document is updated to support a new software release. For example, the first release of a document is 01.01. In the next software release cycle, the first release of the same document is 02.01.

The second two digits indicate the issue. The issue number increases each time the document is revised but rereleased in the same software release cycle. For example, the second release of a document in the same software release cycle is 01.02.

To determine which version of this document applies to the software in your office and how documentation for your product is organized, check the release information in the *UCS DMS-250 Master Index of Publications, 297-2621-001*.

References in this document

The following documents are referred to in this document:

- *DMS-100 DCR User Guide, 297-1001-475*
- *DMS-100 Family Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) Maintenance Guide, 297-2401-502*
- *UCS DMS-250 Billing Records Application Guide, 297-2621-395*
- *UCS DMS-250 Dialable Wideband Services Reference Manual, 297-2621-110*
- *UCS DMS-250 Feature Group D Application Guide, 297-2621-385*
- *UCS DMS-250 FlexDial Framework Application Guide, 297-2621-390*

- *UCS DMS-250 Gateway IMT Application Guide, 297-2621-331*
- *UCS DMS-250 International Application Guide, 297-2621-327*
- *UCS DMS-250 Logs Reference Manual, 297-2621-840*
- *UCS DMS-250 Master Index of Publications, 297-2621-001*
- *UCS DMS-250 Mechanized Calling Card Services (MCCS) Application Guide, 297-2621-305*
- *UCS DMS-250 NetworkBuilder Application Guide, 297-2621-370*
- *UCS DMS-250 PRI RLT Feature Application Guide, 297-2621-347*
- *UCS DMS-250 SS7 RLT Feature Application Guide, 297-2621-345*
- *UCS DMS-250 Transaction Capabilities Application Part (TCAP) Applications Guide, 297-2621-355*

Information about related documents can be found in either the *UCS DMS-250 Master Index of Publications, 297-2621-001*.

What precautionary messages mean

The types of precautionary messages used in NT documents include attention boxes and danger, warning, and caution messages.

An attention box identifies information that is necessary for the proper performance of a procedure or task or the correct interpretation of information or data. Danger, warning, and caution messages indicate possible risks.

Examples of the precautionary messages follow.

ATTENTION - Information needed to perform a task

ATTENTION

If the unused DS-3 ports are not deprovisioned before a DS-1/VT Mapper is installed, the DS-1 traffic will not be carried through the DS-1/VT Mapper, even though the DS-1/VT Mapper is properly provisioned.

DANGER - Possibility of personal injury

DANGER

Risk of electrocution

Do not open the front panel of the inverter unless fuses F1, F2, and F3 have been removed. The inverter contains high-voltage lines. Until the fuses are removed, the high-voltage lines are active, and you risk being electrocuted.

WARNING - Possibility of equipment damage

WARNING

Damage to the backplane connector pins

Align the card before seating it, to avoid bending the backplane connector pins. Use light thumb pressure to align the card with the connectors. Next, use the levers on the card to seat the card into the connectors.

CAUTION - Possibility of service interruption or degradation

CAUTION

Possible loss of service

Before continuing, confirm that you are removing the card from the inactive unit of the peripheral module. Subscriber service will be lost if you remove a card from the active unit.

How commands, parameters, and responses are represented

Commands, parameters, and responses in this document conform to the following conventions.

Input prompt (>)

An input prompt (>) indicates that the information that follows is a command:

```
>BSY
```

Commands and fixed parameters

Commands and fixed parameters that are entered at a MAP terminal are shown in uppercase letters:

```
>BSY CTRL
```

Variables

Variables are shown in lowercase letters:

```
>BSY  CTRL  ctrl_no
```

The letters or numbers that the variable represents must be entered. Each variable is explained in a list that follows the command string.

Responses

Responses correspond to the MAP display and are shown in a different type:

```
FP 3 Busy CTRL 0: Command request has been submitted.

FP 3 Busy CTRL 0: Command passed.
```

1 Software optionality control overview

Introduction

Software Optionality Control (SOC) facilitates the definition and delivery of product computing-module loads (PCLs). All functionality in a PCL is categorized as either base or optional. Base functionality is available immediately after activation. Optional functionality is grouped into commercial units, called SOC options, that can be purchased by operating companies. Options can be ordered, activated, and used without a software reload or restart.

SOC is the tool for managing the options in a PCL. The SOC utility has a user interface for tracking and monitoring optional functions that have been licensed for use on a UCS DMS-250 switch. The SOC user interface consists of command interpreter (CI) commands at the maintenance and administration (MAP) terminal.

The SOC utility provides password protection for SOC-controlled options. Nortel (Northern Telecom) distributes passwords for options that operating companies purchase. A limited number of options are controlled by the SOC utility. For SOC-controlled options, a password is required to change the option's right-to-use (RTU) state, which allows the options to be accessed and activated or deactivated. Most options are only tracked by the SOC utility, which means a password only initiates option visibility on a SOC report.

Password files are transferred using drop boxes, network operations protocol (NOP) links (including X.25), or dial-up modem communication.

More information on the use of SOC passwords is in the Chapter Chapter 2, “SOC quick reference guide."

Note: For a list of UCS DMS-250 SOCs, see Appendix A, “List of UCS DMS-250 SOCs."

Functional overview

SOC has the following capabilities:

- provides an interface through which operating company personnel disable and enable options
- maintains a database of option dependencies to ensure that no option is activated or deactivated without the proper option dependency
- tracks the state of SOC options (ON or IDLE)
- tracks the RTU status of SOC options (YES or NO)
- creates reports containing status information on SOC options
- provides a mechanism for counting and limiting the usage of UCS DMS-250 services and resources
- defines and tracks options not controlled by SOC

Phases of operation

SOC has three phases of operation: software application, restart, and normal operation.

Software application

Software application is the phase during which the PCL is installed on the UCS DMS-250 switch. During a software application, SOC ensures that SOC options in the new software load inherit their settings from the previous software load. After a software application, all SOC options remain in their specified states (ON or IDLE) until a state change is requested through the SOC user interface.

Restarts

During warm and cold restarts, SOC retains its database information, including the states, RTU settings, usage counts, and usage limits of options. However, an option in an error condition that recovers by changing its state during the restart may not return to its original state. In this case, SOC creates a message indicating the new state of the option and why the option's state changed.

Normal operation

During normal operation, SOC periodically audits options to make sure that their current states and usage levels match the states and usage levels recorded for them in the SOC data tables. During these audits, SOC also verifies that dependency requirements for options are being met. SOC also answers queries from other software about the state of options. In addition, operating company personnel can query the status of options on the switch during normal operation.

User queries consist of

- database requests
- RTU or usage limit assignments
- requests to change the usage threshold or the state of an option

Database requests include queries about

- SOC option order codes
- names
- RTU settings
- states
- usage counts
- usage limits

SOC retrieves the data from the SOC database and formats it for output. The user can view the data at the MAP terminal or route the data to a storage file.

SOC options

There are three types of SOC options:

- state
- usage
- dual

State option

A state option has an RTU setting (YES or NO) and a state (ON or IDLE). A user can change the state of an option only if the RTU setting is YES.

The initial RTU for state options can be NO, N/A (not applicable), or A/P (always provided):

- N/A is interpreted as an RTU setting of NO and a state of IDLE (locked).
- A/P is interpreted as an RTU setting of YES (locked) and a state of ON (locked).

Usage option

A usage option has a usage limit (HARD, SOFT, or MONITORED) and a current usage. It has no state and its RTU is determined by its usage limit. If the limit is zero, the RTU is NO; if the limit is greater than zero, the RTU is YES.

Dual option

A dual option has both a usage limit and a state, and its RTU is determined by its usage limit.

LIMIT for a dual option can be any number from 0 to 999999, either HARD or SOFT, MONITORED, N/A, or A/P:

- N/A is interpreted as a hard limit of 0 (locked).
- A/P is interpreted as MONITORED (locked).

Management of SOC options

SOC manages options in three ways. An option can be:

- controlled
- tracked
- pending

SOC controls the state or the usage of controlled options. SOC limits tracked options. SOC only records the RTU settings and usage limits of tracked options. Tracking options allows SOC to provide a complete record of the RTU status of all options in a PCL.

A pending option is a place holder for an option that does not exist in the current software load, but will exist in a future load. Pending options allow the operating company to preconfigure an upcoming option in the on state, or with a certain usage limit. The options in the new load are automatically set to the state or the usage limit assigned to them as pending options. Before the application of the new software load, a pending option with an RTU of YES is configured in the ON state; a pending option with an RTU of NO is configured in the IDLE state.

Key codes

A key code is an alphanumeric password that Nortel gives to the operating company to enable the operating company to assign an RTU setting to an option (granting a key code), remove an RTU from an option (removal of a key code), or assign a new usage limit to an option. Each operation for each option in an office has a unique key code.

What you can do with SOC

The user interface for SOC consists of CI commands at the MAP terminal. The ASSIGN, SELECT, DBAUDIT and REMOVE commands allow you to

- assign the RTU state to an option
- remove the RTU state from an option
- assign a usage limit to an option

- assign RTU states or usage limits to a group of options using a key code file

  Note: See Chapter Chapter 6, “Processing options in a key code file," for more information on key code files.

- assign the ON or IDLE state to an option
- assign a warning threshold to a usage option
- create a report about one or more options in a PCL
- perform an audit of the SOC database

Chapter Chapter 2 is a quick reference guide to the most commonly used SOC commands.

Chapters 11 through 11 contain step-action procedures for the activities listed above. Each procedure is self-contained and provides instructions for logging in and out of SOC. Multiple commands can be entered in the same SOC session, allowing you to perform more than one procedure without logging in and out of SOC between each procedure.

Note: For a list of UCS DMS-250 SOCs, see Appendix A, “List of UCS DMS-250 SOCs."

2 SOC quick reference guide

SOC overview

A software optionality control (SOC) option can be controlled, tracked, or pending. SOC controls the state of controlled options. For tracked options, SOC only monitors and provides reports. A pending option is a place holder for an option that does not exist in the current software load, but is planned for a future load.

SOC options are delivered in product computing-module loads (PCL). SOC options are software-controlled. You need a password to assign right-to-use (RTU) to an option and to activate an option (change from idle state to on state). Tracked options are not software-controlled, but require passwords for visibility of RTU in the SOC utility, and for accurate tracking of licensed software.

SOC options

There are three types of SOC options:

- state option
  - — RTU setting is YES or NO.
  - — State is ON or IDLE.
  - — RTU must be set to YES to change state.
- usage option
  - — has a usage limit of SOFT, HARD, or MONITORED
  - — has a current usage
  - — has no state
  - — RTU is determined by usage limit (RTU is YES for usage limit > 0, RTU is NO for usage limit = 0)
- dual option
  - — has both a usage limit and a state
  - — has RTU determined by usage limit

The initial RTU setting for SOC options can be NO, YES, N/A (not applicable), or A/P (always provided).

The initial RTU for state options can be NO, YES, N/A (not applicable), or A/P (always provided). N/A and A/P are locked settings. For state options, the following applies:

- N/A is interpreted as an RTU setting of NO and a state of IDLE
- A/P is interpreted as an RTU setting of YES and a state of ON

The initial usage limit for a dual option is 0 to 999999, either SOFT or HARD, MONITORED, N/A, or A/P. N/A and A/P are locked settings. For dual options, the following applies:

- an RTU setting of N/A is interpreted as a hard usage limit of 0
- an RTU setting of A/P is interpreted as a usage limit of MONITORED.

The RTU for ordered options is delivered in SOC control files, also known as key codes or password files.

SOC password files

All the passwords required to implement an option are in a single SOC control file. Each SOC control file consists of a file name and one or more password files.

SOC control file format

The following is the format for the SOC control file name:
<switch_id>$<sequence_no>$SCF

where

switch_idis the switch identifier, an alphanumeric character string with up to 11 characters, starting with an alphabetic character.

sequence_nois the four-digit sequence number. If more than one $SCF file exists, the files must be processed according to their sequence number.

The suffix $SCF, which must be present, indicates the file is a SOC control file.

The SOC control file name must not exceed 20 characters.

The NORTEL_ID

- is the first record in the SOC control file
- is a unique identifier assigned to every office, based on the office common language location identifier (CLLI)

- consists of up to 16 uppercase, alphanumeric characters
- is set by the initial SOC control file delivery or password-protected SOC CI command
- requires a patch to change
- transfers during a one-night process (ONP)

See Table Chapter 2, “SOC quick reference guide,” on page -1 Table 2-1, “,” on page 2-3, “Contents of passwords in SOC control files."

Table 2-1

Each password in the SOC control file for	**contains:**
Chapter 2, “SOC quick reference guide,” on page -1Contents of passwords in SOC control files	
a state option	a + or - tag, to indicate whether to grant or revoke the RTU for the option
	a number from 0 to 999999 (or UNLIMITED), to indicate the usage limit setting
	an order code for the option, consisting of eight uppercase, alphanumeric characters
	a 20-character password used to grant RTU for the option
a dual option	a + or - tag, to indicate whether to grant or to revoke the RTU for the option
	a number from 0 to 999999, to indicate a hard usage limit setting
	a number from 0 to 999999 followed by an S, to indicate a soft usage limit setting
	MONITORED, to indicate a non-limited usage option
	an order code for the option consisting of eight uppercase, alphanumeric characters
	a 20-character password used to grant RTU for the option

SOC Communication Protocol

The SOC Communication Protocol (SOCCOM) feature provides the capability for remote access to the SOC application on the UCS DMS-250 switch. SOCCOM allows Nortel and operating company personnel at the remote network operations system (NOS) to apply SOC key codes to and collect SOC option reports from the UCS DMS-250 switch.

SOCCOM is a network operations protocol (NOP) application that acts as an interface between the UCS DMS-250 SOC application and the remote application on the NOS. SOCCOM provides the following functionality:

- version control, to ensure the corresponding releases of the remote SOC and the UCS DMS-250 SOC applications are in use
- the capability to query and set the NORTEL_ID office parameter
- interactive communication between the remote user and the UCS DMS-250 SOC application for the following commands:
  - — ASSIGN KEYS (used to turn features on or off)

    Note: For more information on the assign keys command, see Chapter Chapter 6, “Processing options in a key code file."

  - — SELECT ALL PACK (used to display information about SOC options)

    Note: For more information on the select all command, see Chapter Chapter 9, “Creating a SOC report."

Activating the SOC Communication Protocol feature

SOCCOM is activated in table NOPAPPLN by changing the appropriate tuple, indexed by the directory number address (DNA) key (field DNAKEY), so that the SOCCOM application is enabled for the DNA.

See Table Chapter 2, “SOC quick reference guide,” on page -1 Table 2-2, “,” on page 2-4, “Refinement CHOICE value."

Table 2-2

If the value of refinement CHOICE in field APPLNS is:	**then:**
Chapter 2, “SOC quick reference guide,” on page -1Refinement CHOICE value	
ALL	all applications are valid and no datafill change is required
ONLY	SOCCOM must be added to the tuple

To activate SOCCOM, perform this procedure at the MAP terminal:

1 Access table NOPAPPLN:

```
>TABLE NOPAPPLN
```

Response example:
Table:NOPAPPLN

2 List the tuples in the table:

```
>LIS ALL
```

Response example:
DNAKEY
APPLNS

9040001105 ALL
9040001106
ONLY (FTRAN) (PTAE_APPL) $

3 Activate SOCCOM for the DNA:

```
>CHA APPLNS ONLY appln1 appln2 SOCCOM $
```

where

appln1
is the first application associated with the DNA

appln2
is the second application associated with the DNA

Note: The values appln1 and appln2 represent the applications associated with the DNA. You can enter one or more applications in the command string.

Input example:

```
>CHA APPLNS ONLY FTRAN PTAE_APPL SOCCOM $
```

Response example:
TUPLE TO BE CHANGED:
904001106
ONLY (FTRAN) (PTAE_APPL) (SOCCOM) $
ENTER Y TO CONFORM, N TO REJECT, E TO EDIT

4 Confirm the command:

```
>Y
```

Response example:
TUPLE CHANGED
JOURNAL FILE INACTIVE

5 Quit from table NOPAPPLN:

```
>QUIT
```

SOC commands

Table Chapter 2, “SOC quick reference guide,” on page -1 contains brief descriptions of the SOC commands. Each description identifies the chapter in this book that contains detailed instructions for using the command.

Table 2-3 (Sheet 1 of 2)

Command	Description	Related chapter
Chapter 2, “SOC quick reference guide,” on page -1SOC commands		
ASSIGN	used to	
	• assign option order codes from a file	Chapter Chapter 6, “Processing options in a key code file"
	• assign a key code to a SOC option	
	• assign a new state to a state or dual option	Chapter Chapter 7, “Changing the state of an option"
	• assign a usage limit to a usage or dual option	Chapter Chapter 5, “Assigning a usage limit to an option"
	• assign a warning threshold to a usage or dual option	Chapter Chapter 8, “Assigning a warning threshold to an option"
	• assign RTU to an option	Chapter Chapter 3, “Assigning right to use to an option"
	• remove RTU from an option	
DBAUDIT	used to audit SOC data and report any inconsistencies.	Chapter Chapter 10, “Auditing the SOC database"
HELP	used to display information on SOC commands	none
Q	used to display information on SOC commands	none
QUIT	used to quit from the SOC utility	none
REMOVE	used to remove RTU from an option	Chapter Chapter 4, “Removing RTU from an option"
SELECT	used to display information on SOC options	Chapter Chapter 9, “Creating a SOC report"

Table 2-3 (Sheet 2 of 2)

Command	Description	Related chapter
SOC	used to access the SOC utility	none
SOCDEBUG	used to access the SOC debug utility. The SOC debug utility is only for use by Nortel field support.	none
VALIDATE	To the extent that it is possible to do so without activating or deactivating any functionality, this command determines if a SOC option state transition would be successful. ***Note:*** Even if the VALIDATE command returns a pass or fail result, there is no guarantee that the indicated state transition will succeed or fail.	none

Verifying the content of SOC control files

SOC control files can contain more SOC option order codes than are ordered. Unordered SOC options are the result of dependencies for ordered options.

Note: SOC control files are delivered by one of the following methods:

- downloaded by Nortel to SFDEV
- distributed by the telephone company

To verify the contents of SOC control files, perform the following procedure at the MAP terminal:

To verify the contents of SOC control files, perform the following procedure at the MAP terminal:

1 Access the disk utility:

```
>DISKUT
```

2 List the files in the volume where the SOC control file is stored:

```
>LF volume_name
```

where

volume_name
is the system load module disk volume

Input example:

```
>LF S00DAS0C
```

Response example:
File information for volumed SOODIMAGE1:
{NOTE: 1 BLOCK = 512 BYTES }

```
-------------------------------------------------------------
FILE NAMEO  R  I  O  O  O  FILE MAX NUM OFFILE LAST
R  E  T  P  L  L  CODE REC RECORDSSIZE MODIFY
G  C  O  E  D  D       LEN      IN  IN DATE
 C  N  FILE BLOCKS
-------------------------------------------------------------
DOLISTO  V 0 128   6015 950811
A12DS0$0001$SCFO  V 0 128   3315 950811
KWH16IB5$PATCHO  V 0 128   3115 950728
AUTOSCHEDO  V 0 128   3215 950802
```

Note: In the above example, the SOC control file is A12DS0$0001$SCF and has been deposited in system load module disk volume s00dasoc.

3 Quit the disk utility:

```
>QUIT
```

4 Print the contents of the volume:

```
>RECORD START ONTO printer
```

where

printer
is the name of the printer on which you are printing

Input example:

```
>RECORD START ONTO MPS26D13C
```

Response example:
DONE

5 Print the SOC control file:

```
>PRINT file_name
```

where

file_name
is the name of the SOC control file

Input example:

```
>PRINT A12DS0$0001$SCF
```

Response example:
A12DS0$0001$

+ RES00012 DQW9X3UZ9VEAK4A2851R

where

A12DS0
is the switch identifier

RES00012
is the SOC order code

Note: Each record has the format *<+, -><soc_order_code><soc_key>*. Usually, the first field is +, indicating the RTU for the field is to be set to YES. If this field is -, the RTU is to be set to NO.

6 Compare the contents of the SOC control file to your order.

7 Reconcile any differences. If you find any differences between your order and the SOC control file, contact your Nortel customer service representative.

Assigning RTU and activating SOC options

ATTENTION

When the SOC control file delivery is the first for an office, the control file and the ASSIGN KEYS command must be used to establish the NORTEL_ID. If the SOC control file is not used to establish the NORTEL_ID, the NORTEL_ID is undefined, and the operating company is not able to install or activate SOC.

To assign RTU and activate SOC options, perform the following procedure at the MAP terminal:

To assign RTU and activate SOC options, perform the following procedure at the MAP terminal:

1 Enter the SOC utility:

```
>SOC
```

2 Assign RTU and usage limits to options in the SOC control file:

```
>ASSIGN KEYS FROM FILE
```

Responses:

The system searches for all files with the $SCF suffix. All devices in table PADNEV (patch administration and downloading device) and then SFDEV are searched.

If the system finds a single $SCF file, it processes the file. Continue with step 5.

If the system finds more than one $SCF file, it fails to process the file and gives the following response:

SOC status reports

You can create the following types of SOC reports:

- brief
  - — shows the basic RTU, state, usage, last change date, and type information for options
- pack
  - — shows the content of the brief report, but all extra spaces are deleted
- verbose
  - — shows the content of the brief report; also shows option dependencies (needed options and mutually exclusive options), thresholds, feature usage counts for usage and dual options, and high water marks
- full
  - — shows the content of the verbose report; also shows the feature identifiers, feature names, feature states, and the last change dates for included features

Feature usage counts are not set to zero (0) during restarts.

For detailed information and instructions on SOC reports, refer to Chapter Chapter 9, “Creating a SOC report."

3 Assigning right-to-use (RTU) to an option

When you purchase a state option, Nortel gives your company a password called a key code for the state option. Once you have the key code, you can use the ASSIGN RTU command. The ASSIGN RTU command allows you to change the option's state.

You can assign the right-to-use (RTU) state to a group of options by applying the ASSIGN KEYS command to a key code file. This file, supplied by Nortel, contains a list of order codes and key codes for the options. Chapter Chapter 3 describes how to assign the RTU state and usage limits to, or remove the RTU state from, a group of options in a key code file.

The ASSIGN RTU command can be used with state options only. The RTU state of usage and dual options is controlled by assigning a usage limit to the option. Chapter Chapter 5 describes how to assign a usage limit to an option.

The following procedure describes how to assign the RTU state to a single option. Software optionality control (SOC) creates a SOC504 log if the RTU application is successful, and a SOC505 log if the RTU application is not successful.

Procedure 3-1 Replacing a/an <PEC or card type> in <shelf or context>

Assigning the RTU state to an option

1 Access the SOC directory by typing

>SOC

See Table 3 3-1, “System response when accessing the SOC directory."

Table 3-1 System response when accessing the SOC directory

If the system response is	Do	Reason
`User count exceeded; SOC in use by <user>`	step 2	Only one SOC session at a time can be active. The user ID of the user running the other session is shown in the response.
`SOC is already running`	step 3	Your CI session already has a SOC session running.
`SOC cannot be used while a dump is in progress. SOC not started`	step 4	SOC cannot start because the system is performing an image dump.
`The SOC prompt`	step 5	You have started a SOC session.
`Couldn't allocate SOC command directory...SOC not started`	step 9	SOC cannot allocate the SOC directory because the FuncGrp office has a resource problem.
`Couldn't allocate mailboxes...SOC not started`	step 9	SOC cannot allocate its mailboxes because the FuncGrp office has a resource problem.
Note: For assistance, contact the personnel responsible for your next level of support.		

2 See Table 3 3-2, “Steps to follow when 'User count exceeded' appears."

Table 3-2 ***Steps to follow when “User count exceeded" appears***

If	then
you are certain that no other SOC session is running	reset the usage counter for the SOC session. ***Note:*** For assistance, contact the personnel responsible for your next level of support.
another SOC session is running	wait for the other SOC session to terminate and then go to step 1.

3 Wait for the other SOC session to terminate and then go to step 1.

4 Wait for the image dump to complete and then go to step 1.

5 To set the right-to-use (RTU) to YES for an option or to create a pending option, enter the ASSIGN RTU command by typing

```
>ASSIGN  RTU  key_code  TO  order_code
```

where

key_code is the granting key code (20 alphanumeric characters), supplied by Nortel

order_code is the order code (8 alphanumeric characters), assigned by Nortel

Input example:

```
>ASSIGN  RTU  KDLAS43895JFKDNWMKCM  TO  CTX00001
```

6 See Table 3 3-3, “System response to ASSIGN RTU command."

Table 3-3 (Sheet 1 of 3)

If the system response is	Do	Reason
3System response to ASSIGN RTU command		
`Illegal order code <code>`	step 5	The string you entered is not a valid order code.
Note: For assistance, contact the personnel responsible for your next level of support.		

Table 3-3 (Sheet 2 of 3)

If the system response is	Do	Reason
`Unknown order code <code> (or wrong key code for new option)`	step 7	If you are trying to create a pending option, this message indicates that the key code is not valid for the option. If you are trying to assign RTU to an existing option, this message indicates that SOC does not have a record of the specified order code.
`Option <order code> is N/A (not applicable|A/P (always provided). Its <RTU|limit|state> cannot be changed.`	step 7	The option is designated as not applicable (N/A) or always provided (A/P). You cannot change the option's RTU state.
`Cannot set RTU for usage or dual option`	step 7	The RTU for this option cannot be set because the option is a usage or dual option, not a state option.
`Incorrect key code for option`	step 8	The key code you entered is incorrect for the option.
`Incorrect key code for option but the right-to-use was already set, so changes are allowed`	step 9	You have entered an incorrect key code for the option; the RTU, however, was already set to YES for the specified option.
Note: For assistance, contact the personnel responsible for your next level of support.		

Table 3-3 (Sheet 3 of 3)

If the system response is	Do	Reason
`Pending option <order code> created`	step 9	A pending option has been created and the RTU for that option has been set to YES.
`Done`	step 9	The ASSIGN RTU command was successful. Either the RTU for the option has been set to YES or a pending option has been created.
Note: For assistance, contact the personnel responsible for your next level of support.		

7 Check that you have entered the correct order code. If you have not, go to step 5.

Note: For assistance, contact the personnel responsible for your next level of support.

8 Check that you have entered the correct key code and order code. If you have not, go to step 5.

Note: For assistance, contact the personnel responsible for your next level of support.

9 Exit the SOC directory by typing

```
>QUIT
```

4 Removing RTU from an option

The ASSIGN RTU command allows you to remove the right-to-use (RTU) state from a state option. Removing the RTU state from an option prevents subsequent state changes for that option.

> ***Note:*** Although you can use the REMOVE RTU command to remove the RTU state from a state option, you should use the ASSIGN RTU command. The REMOVE RTU command is redundant.

An option that is controlled by software optionality control (SOC) must be in the idle state before you can remove its RTU state. You can remove the RTU for a tracked option or a pending option at any time.

The ASSIGN RTU command applies to state options only. To achieve the same functionality for a usage or dual option, assign a usage limit of zero, as described in Chapter Chapter 5, “Assigning a usage limit to an option."

The following procedure explains how to remove the RTU from a state option. If the procedure is successful, SOC creates a SOC504 log. If the procedure is not successful, SOC creates a SOC505 log.

Removing the RTU state from an option

1 Access the SOC directory by typing

>SOC

See Table 4-1, System response when accessing the SOC directory.

Table 4-1 System response when accessing the SOC directory

If the system response is	Do	Reason
`User count exceeded; SOC in use by <user>`	step 2	Only one SOC session at a time can be active. The user ID of the user running the other session is shown in the response.
`SOC is already running`	step 3	Your CI session already has a SOC session running.
`SOC cannot be used while a dump is in progress. SOC not started`	step 4	SOC cannot start because the system is performing an image dump.
`The SOC prompt`	step 5	You have started a SOC session.
`Couldn't allocate SOC command directory...SOC not started`	step 11	SOC cannot allocate the SOC directory because the FuncGrp office has a resource problem.
`Couldn't allocate mailboxes...SOC not started`	step 11	SOC cannot allocate its mailboxes because the FuncGrp office has a resource problem.

2 See Table 4-2, “Steps to follow when 'User count exceeded' appears."

Table 4-2 Steps to follow when “User count exceeded" appears (Sheet 1 of 2)

If	then

Table 4-2 Steps to follow when “User count exceeded" appears (Sheet 2 of 2)

you are certain that no other SOC session is running	reset the usage counter for the SOC session. ***Note:*** For assistance, contact the personnel responsible for your next level of support.
another SOC session is running	wait for the other SOC session to terminate and then go to step 1.

3 Wait for the other SOC session to terminate and then go to step 1.

4 Wait for the image dump to complete and then go to step 1.

5 To remove the RTU from an option, enter the ASSIGN RTU command by typing

```
>ASSIGN  RTU  key_code  TO  order_code
```

where

key_code is the removal key code (20 alphanumeric characters) supplied by Nortel

order_code is the order code (8 alphanumeric characters) assigned by Nortel

Example input

```
>ASSIGN  RTU  KDLAS43895JFKDNWMKCM  TO  CTX00001
```

6 See Table 4-3, “System response to the ASSIGN RTU command."

Table 4-3 *System response to the ASSIGN RTU command* (Sheet 1 of 2)

If the system response is	Do	Reason
`Unknown order code <code>`	step 1	SOC does not have a record of the specified order code.
`Illegal order code <code>`	step 1	The string you entered is not a valid order code.
Note: For assistance, contact the personnel responsible for your next level of support.		

Table 4-3 ***System response to the ASSIGN RTU command*** **(Sheet 2 of 2)**

If the system response is	Do	Reason
`Option <order code> is N/A (not applicable|A/P (always provided). Its <RTU|limit|state> cannot be changed.`	step 1	The option is designated as not applicable (N/A) or always provided (A/P). You cannot change the option's RTU state.
`Cannot revoke RTU when state is not IDLE`	step 1	The option is in the ON state and, therefore, the RTU state for that option cannot be removed.
`Incorrect key code for option`	step 1	The key code you entered is incorrect.
Cannot set RTU for usage or dual option	step 1	You have tried to remove the RTU for a usage or dual option. To remove the RTU for a usage or dual option, you must set the usage limit to 0.
`Done`	step 1	The ASSIGN RTU command was successful. The RTU state for the option has been removed.
Note: For assistance, contact the personnel responsible for your next level of support.		

7 Check that you have entered the correct order code. If you have not, go to step 1.

Note: For assistance, contact the personnel responsible for your next level of support.

8 Follow the procedure in Chapter 7 to change the state of the option to idle, and then go to step 6.

Note: For assistance, contact the personnel responsible for your next level of support.

9 Check that you have entered the correct key code and order code. If you have not, go to step 5.

Note: For assistance, contact the personnel responsible for your next level of support.

10 Follow the procedure in Chapter 5 to set the usage limit to 0 and then go to step 11.

11 Exit the SOC directory by typing

```
>QUIT
```

5 Assigning a usage limit to an option

Usage limits allow you and Nortel to control the amount of resources or services that are being used. Defining usage limits is part of the contractual arrangement between Nortel and your operating company. Usage limits are controlled by key codes, which are passwords distributed by Nortel. See Chapter Chapter 6, “Processing options in a key code file," for more information on key codes. Software optionality control (SOC) records a current usage and a high water mark in units defined by the option for each usage option and dual option. The record is available to your operating company in SOC reports and is used as input to Nortel for billing purposes.

Assigning usage limits to options

When you set usage limits, you can set a soft limit or a hard limit for each option, or you can specify that the option be monitored. When a hard limit is reached, no more of the option's resources can be allocated; SOC creates a log stating that a hard limit has been reached. When a soft limit is reached, SOC creates a log, but the option's resources can still be allocated. SOC records the usage level but does not limit the usage of a monitored option.

Controlling the RTU of usage options

Setting the usage limit controls the right-to-use (RTU) for usage and dual options. The RTU is YES if you assign a usage limit greater than zero. The RTU is NO if you assign a usage limit of zero.

The following procedure explains how to assign a usage limit to an option. SOC creates a SOC504 log if the procedure is successful, and a SOC505 log if the procedure is not successful.

Procedure 5-1 Procedure for assining a usage limit to an option

1 Access the SOC directory by typing

>SOC

See Table 5-1, “System response when accessing the SOC directory."

Table 5-1 System response when accessing the SOC directory

If the system response is	Do	Reason
`User count exceeded; SOC in use by <user>`	step 2	Only one SOC session at a time can be active. The user ID of the user running the other session is shown in the response.
`SOC is already running`	step 3	Your CI session already has a SOC session running.
`SOC cannot be used while a dump is in progress. SOC not started`	step 4	SOC cannot start because the system is performing an image dump.
`The SOC prompt`	step 5	You have started a SOC session.
`Couldn't allocate SOC command directory...SOC not started`	step 11	SOC cannot allocate the SOC directory because the FuncGrp office has a resource problem.
`Couldn't allocate mailboxes...SOC not started`	step 11	SOC cannot allocate its mailboxes because the FuncGrp office has a resource problem.

2 See Table 5-2, “Steps to follow when 'User count exceeded' appears."

Table 5-2 Steps to follow when “User count exceeded" appears (Sheet 1 of 2)

If	then

Table 5-2 Steps to follow when “User count exceeded" appears (Sheet 2 of 2)

If	then
you are certain that no other SOC session is running	reset the usage counter for the SOC session. ***Note:*** For assistance, contact the personnel responsible for your next level of support.
another SOC session is running	wait for the other SOC session to terminate and then go to step 1.

3 Wait for the other SOC session to terminate and then go to step 1.

4 Wait for the image dump to complete and then go to step 1.

5 To assign a usage limit to an option or to create a pending option, enter the ASSIGN LIMIT command by typing

```
>ASSIGN  LIMIT  limit  key_code  TO  order_code
```

where

limit is the new limit value for the option (number between 0 and 999999 or MONITORED)

key_code is the key code assigned by Nortel (20 alphanumeric characters), for setting a usage limit for the option

order_code is the order code (8 alphanumeric characters) assigned by Nortel

Note: MONITORED in the limit field specifies that SOC does not restrict the usage of the option.

Input example

```
>ASSIGN  LIMIT  1945  ABCDABCDABCDABCDABCD  TO  CTX00001
```

6 See Table 5-3, “System response to ASSIGN LIMIT command."

Table 5-3 System response to ASSIGN LIMIT command (Sheet 1 of 3)

If the system response is	Do	Reason
`Illegal order code <code>`	step 7	The string you entered is not a valid order code.
Note: For assistance, contact the personnel responsible for your next level of support.		

Table 5-3 System response to ASSIGN LIMIT command (Sheet 2 of 3)

If the system response is	Do	Reason
`Unknown order code <code> (or wrong key code for new option)`	step 7	If you are trying to create a pending option, this response indicates that the key code is not valid for the option. If you are trying to assign a usage limit to an existing option, this response indicates that SOC does not have a record of the specified order code.
`Option <order code> is N/A (not applicable|A/P (always provided). Its <RTU|limit|state> cannot be changed.`	step 7	The option is designated as not applicable (N/A) or always provided (A/P). You cannot change the option's RTU state.
`Cannot set limit for state option`	step 7	You have tried to assign a usage limit to a state option.
`Illegal limit (must be 0<=limit<=999999)`	step 8	You have entered an incorrect usage limit. The usage limit must be a number between 0 and 999999 or the word MONITORED.
`Cannot set limit to zero because option state is not IDLE`	step 9	The state of a dual option must be IDLE before you can set the limit for that option to zero (0).
`Incorrect key code for option`	step 10	You have specified an incorrect key code for assigning a usage limit to the option.
Note: For assistance, contact the personnel responsible for your next level of support.		

Table 5-3 System response to ASSIGN LIMIT command (Sheet 3 of 3)

If the system response is	Do	Reason
`Done<Warnings>`	step 11	The ASSIGN LIMIT command was successful. You have assigned a usage limit to the option, have set the usage limit of the option to MONITORED, or have created a pending option. The response may include information messages.
`SSP routeset limit must be 1 less than a multiple of 256.`	step 11	The routeset limit must be one less than a multiple of 256 (that is, 255, 511, 767, 1023, 1279, 1535, 1791, or 2047).
`Maximum supported SSP routeset limit is 255 tuples.`	step 11	If the tuple is added, the limit for routesets with external routing off will be exceeded.
`Maximum supported SSP routeset limit is 2047 tuples.`	step 11	If the tuple is added, the limit for routesets with external routing on will be exceeded.
Note: For assistance, contact the personnel responsible for your next level of support.		

7 Check that you have entered the correct order code. If you have not go to step 5.

Note: For assistance, contact the personnel responsible for your next level of support.

8 Check that you have entered the correct usage limit. If you have not go to step 5.

Note: For assistance, contact the personnel responsible for your next level of support.

9 Follow the procedure in Chapter 7 to change the state of the option to idle and then go to step 5.

Note: For assistance, contact the personnel responsible for your next level of support.

10 Check that you have entered the correct key code and order code. If you have not, go to step 5.

Note: For assistance, contact the personnel responsible for your next level of support.

11 Exit the SOC directory by typing

```
>QUIT
```

6 Processing options in a key code file

Nortel sets up the key code file, which contains a list of order codes and key codes. This file allows you to assign the right-to-use (RTU) settings and usage limits to a group of options, instead of processing each option individually.

The following procedure explains how to apply key codes to a set of options. Software optionality control (SOC) creates a SOC504 log for each successful key code application, and a SOC505 log for each unsuccessful one.

Processing options in a key code file

1 Access the SOC directory by typing

>SOC

See Table 6-1, “System response when accessing the SOC directory."

Table 6-1 (Sheet 1 of 2)

If the system response is	Do	Reason
System response when accessing the SOC directory		
`User count exceeded; SOC in use by <user>`	step 2	Only one SOC session at a time can be active. The user ID of the user running the other session is shown in the response.
`SOC is already running`	step 3	Your CI session already has a SOC session running.
`SOC cannot be used while a dump is in progress. SOC not started`	step 4	SOC cannot start because the system is performing an image dump.
`The SOC prompt`	step 5	You have started a SOC session.

Table 6-1 (Sheet 2 of 2)

If the system response is	Do	Reason
`Couldn't allocate SOC command directory...SOC not started`	step 9	SOC cannot allocate the SOC directory because the FuncGrp office has a resource problem.
`Couldn't allocate mailboxes...SOC not started`	step 9	SOC cannot allocate its mailboxes because the FuncGrp office has a resource problem.

2 See Table 6-2, “Steps to follow when 'User count exceeded' appears."

Table 6-2

Steps to follow when “User count exceeded" appears	
If	then
you are certain that no other SOC session is running	reset the usage counter for the SOC session. ***Note:*** For assistance, contact the personnel responsible for your next level of support.
another SOC session is running	wait for the other SOC session to terminate and then go to step 1.

3 Wait for the other SOC session to terminate and then go to step 1.

4 Wait for the image dump to complete and then go to step 1.

5 See Table 6-3, “Steps to follow after starting a SOC session."

Table 6-3

If you are	Do
Steps to follow after starting a SOC session	
accepting the default file name and default device	step 6
specifying a file name and device	step 8
specifying a file name and accepting the default device	step 9

Note: We recommend that you use the default file name and device; however, SOC capability enables you to specify your own file name and device.

6 To assign RTU and usage limits to options in a file with the default file name and default device, enter the ASSIGN KEYS command by typing

>ASSIGN KEYS FROM FILE

See Table 6-4, “System response to the ASSIGN KEYS command when using the default file name and default device."

Table 6-4

If the response is	Do
System response to the ASSIGN KEYS command when using the default file name and default device	
`Failed: No KEYS were assigned.More than one $SCF file was found.`	step 7
anything else	step 10

7 Assign RTU and usage limits to the file with the lowest sequence number by typing

>ASSIGN KEYS FROM filename

Note: The default file name has the format <switch_id>$<sequence_no>$SCF, where switch_id is the switch identifier, sequence_no is the $SCF file sequence number, and the file is located on one of the volumes in the patch administration and downloading device (PADNDEV) table or on SFDEV.

Repeat step 7 for each of the remaining $SCF files and then go to step 10.

Note: The $SCF files must be processed according to their sequence number.

8 To assign RTU and usage limits to options in a file whose name and device you are specifying, enter the ASSIGN KEYS command by typing

>ASSIGN KEYS FROM filename device

where

filename iis an alphanumeric name of a file, supplied by Nortel, that lists order codes and corresponding key codes

device is the alphanumeric name of the device that contains the volume that contains the file

Input example:

>ASSIGN KEYS FROM OTWAONXBD50 SFDEV

Go to step 10.

9 To assign RTU and usage limits to options in a file when you are specifying the file name and accepting the default device, enter the ASSIGN KEYS command by typing

>ASSIGN KEYS FROM filename

where

filename is an alphanumeric name of a file, supplied by Nortel, that lists order codes and corresponding key codes

Example input

>ASSIGN KEYS FROM OTWAONXBD50

Go to step 10.

10 See Table 6-5, System response to the ASSIGN KEYS command when specifying the file name and accepting the default device.

Table 6-5

If the system response is	Do	Reason
System response to the ASSIGN KEYS command when specifying the file name and accepting the default device		
`<error summary> Done <n> errors detected. File not erased`	step 11	The response is a summary of the errors SOC found while processing the key code file. Order codes associated with an error may not have been processed.
`Done`	step 15	The ASSIGN KEYS command was successful. The RTU and usage limit requests for all options in the file have been processed, and the file was deleted.

11 Review the key code file to determine the errors and then see Table 6-6 , Steps to follow when you receive error messages.

Table 6-6 (Sheet 1 of 3)

If the system response is	Do	Reason
Steps to follow when you receive error messages		
`Cannot revoke RTU in file state is not IDLE in file <file> at line <line number>`	step 12	SOC found an option in the on state in the key code file and, therefore, the RTU for that option cannot be removed.
`Cannot find file <filename> on device <device>`	step 13	SOC could not find the key code file on the device displayed in the error message.
`Cannot find file <filename> on any device in table PADNDEV`	step 13	SOC could not find the key code file on any devices listed in table PADNDEV.
`Syntax error in <file name> at <line number>`	step 14	The system cannot interpret one of the lines in the file. The file name and line number are provided in the error message.
`Incorrect CLLI in <filename> at line 1`	step 14	The NORTEL_ID on the first line of the file does not match the NORTEL_ID for your office as specified in table OFCSTD.
Note 1: More than one of these error messages may appear. If there are more than one error messages, take appropriate action for each error before you go to step 15.		
Note 2: For assistance contact the personnel responsible for the next level of support.		

Table 6-6 (Sheet 2 of 3)

If the system response is	Do	Reason
`Unknown key code tag (should be +,- or a limit) in <filename> at line <linenum>`	step 14	SOC found an incorrect grant character, revoke character, or limit in the key code file. The option with the order code associated with that key code is not processed and the file is not deleted. All options without errors in the key code file are processed.
`Unknown order code <code> (or wrong key code for new option) in file <file> at line <line number>`	step 14	Either the key code is not valid for creating a pending option or SOC does not have a record of the order code. The file name and line number of the unknown order code are displayed in the error message.
`Illegal order code <code> in file <file> at line <line number>`	step 14	SOC found an order code with invalid syntax in the key code file. The file name and line number of the invalid order code are displayed in the error message.
`Incorrect key code for option in file <file name> at line <line number>`	step 14	SOC found an incorrect key code in the key code file. The file name and line number of the incorrect key code, and its corresponding order code, are displayed in the error message.
Note 1: More than one of these error messages may appear. If there are more than one error messages, take appropriate action for each error before you go to step 15. ***Note 2:*** For assistance contact the personnel responsible for the next level of support.		

Table 6-6 (Sheet 3 of 3)

If the system response is	Do	Reason
`File processing error: couldn't open <filename>`	step 14	SOC could not open the key code file. Either the file is open for another process or there is a file system failure.
`File processing error: couldn't read <filename>`	step 14	SOC found an error while reading the key code file. If at least one line has been read by SOC, the message displays the number of the line with the error. Either the file is incorrectly formatted or the physical device has a problem.
`File processing error: couldn't close <filename>`	step 15	SOC processed the key code file but could not close it. The message shows the name of the file. SOC exits the file without deleting it. If no other error conditions exist, the RTU and usage limit requests for all options in the file have been processed.
`File processing error: couldn't erase <filename>(but key codes were applied successfully)`	step 15	SOC processed the key code file but could not delete it. The message shows the name of the file. If no other error conditions exist, the RTU and usage limit requests for all options in the file have been processed.
Note 1: More than one of these error messages may appear. If there are more than one error messages, take appropriate action for each error before you go to step 15. ***Note 2:*** For assistance contact the personnel responsible for the next level of support.		

12 Change the state of the option to idle by following the procedure in Chapter 7 and remove the RTU for that option by following the procedure in Chapter 4, and then return to this point.

If there are other error messages, take appropriate action; otherwise, go to step 15.

13 Ensure that the file name is correct and that the file resides on the specified device. If the file and device name are incorrect, go to step 9.

Note: For assistance contact the personnel responsible for the next level of support.

14 For assistance fixing errors that SOC found while processing the ASSIGN KEYS command, contact the personnel responsible for the next level of support.

When you have corrected the problem in the error message that sent you to this step, address the next error message. When all problems have been corrected, go to step 15.

15 Exit the SOC directory by typing

```
>QUIT
```

7 Changing the state of an option

Option states

Software optionality control (SOC) allows you to activate an option (assign the ON state) and to deactivate an option (assign the IDLE state). In the ON state, an option is fully operational; in the IDLE state, an option cannot be used. Some options retain datafill in the IDLE state. Other options can have datafill in the ON state only; for these options, datafill must be removed before the option can be set to IDLE. Usage options do not have a SOC state.

Once an operating company purchases an option, receives the key code for the option, and assigns the right-to-use (RTU) to the option, the option can be activated and deactivated without Nortel involvement. When you activate an option, SOC verifies the RTU setting is YES before allowing the option to change states. When you deactivate an option, SOC displays messages, if there are any, describing the impact of deactivating the option, and prompts you either to confirm or to cancel the request. After the option is deactivated, it is not operational.

The following procedure provides instructions on how to change the state of an option. SOC creates a SOC501 log if the option successfully changes state. SOC creates a SOC503 log, and possibly a SOC502 log, if the option does not change state. A SOC502 log indicates which feature in the option caused the failure.

Assigning a state to an option

1 Access the SOC directory by typing

>SOC

See Table 7-1, “System response when accessing the SOC directory."

Table 7-1

If the system response is	Do	Reason
System response when accessing the SOC directory		
`User count exceeded; SOC in use by <user>`	step 2	Only one SOC session at a time can be active. The user ID of the user running the other session is shown in the response.
`SOC is already running`	step 3	Your CI session already has a SOC session running.
`SOC cannot be used while a dump is in progress. SOC not started`	step 4	SOC cannot start because the system is performing an image dump.
`The SOC prompt`	step 5	You have started a SOC session.
`Couldn't allocate SOC command directory...SOC not started`	step 1	SOC cannot allocate the SOC directory because the FuncGrp office has a resource problem.
`Couldn't allocate mailboxes...SOC not started`	step 1	SOC cannot allocate its mailboxes because the FuncGrp office has a resource problem.

2 See Table 7-2, “Steps to follow when 'User count exceeded' appears."

Table 7-2 (Sheet 1 of 2)

Steps to follow when “User count exceeded" appears	
If	then

Table 7-2 (Sheet 2 of 2)

you are certain that no other SOC session is running	reset the usage counter for the SOC session. ***Note:*** For assistance, contact the personnel responsible for your next level of support.
another SOC session is running	wait for the other SOC session to terminate and then go to step 1.

3 Wait for the other SOC session to terminate and then go to step 1.

4 Wait for the image dump to complete and then go to step 1.

5 To change the state of an option, enter the ASSIGN STATE command by typing

```
>ASSIGN  STATE  state  TO  order_code
```

where

state is the state to which you want to change the option (IDLE or ON)

order_code is the order code (8 alphanumeric characters), assigned by Nortel

Example input

```
>ASSIGN  STATE  ON  TO  CTX00001
```

See Table 7-3, “System response to the ASSIGN STATE command."

Table 7-3 (Sheet 1 of 2)

If the system response is	Do	Reason
System response to the ASSIGN STATE command		
`<impact statement> Confirm change of option <order code> to state <state> by entering the textual option name`	step 1	Describes the impact of changing the state of the option to IDLE and displays a prompt for the textual name of the option.
`Unknown order code <code>`	step 1	SOC does not have a record of the specified order code.
`Illegal order code <code>`	step 1	The string you entered is not a valid order code.

Table 7-3 (Sheet 2 of 2)

If the system response is	Do	Reason
`Illegal to assign state to usage-only option`	step 1	The state change for the option cannot be processed because the option is a usage option.
`Illegal to assign state to tracked or pending option`	step 1	The state change cannot be processed because the option is a tracked or pending option.
`Right-to-use not granted`	step 1	The RTU state has not been set to YES for this option.
`<validation errors> Transition refused, because of validation errors`	step 1	The state change for the option has not been allowed because all or part of the option is unable to change state.
`<failure reasons> Transition failed. Option is in state <state>`	step 1	The attempt to change the state of the option failed. The response displays the reason for the failure, how to fix the problem, and the current state of the option. The current state of the option will be one of on, idle, on-to-idle and idle-to-on. On-to-idle and idle-to-on are transitional states; if an error occurs during the state transition and the option can neither revert to its previous state nor change to the new one, the option will be in either the on-to-idle or the idle-to-on state.
`Done`	step 1	The ASSIGN STATE command was successful. The option has been changed to the specified state.

6 Read the messages and determine whether or not you want to proceed with the request to change the state of the option. See Table 7-4, Steps to follow after determining whether to change the state of the option.

Table 7-4

If you	Do
Steps to follow after determining whether to change the state of the option	
want to change the state of the option	step 1
do not want to change the state of the option	step 1

7 Type the textual name of the option. See Table the state of the option."

Table 7-5

If the system response is	Do	Reason
System response when changing the state of the option		
`Too many tries. Command cancelled`	step 1	The system terminated processing because you entered an incorrect textual name three times.
`Done`	step 1	The ASSIGN STATE command was successful. The option has been changed to the specified state.

8 To determine the correct textual name for the option, create a brief report for the option by typing

```
>SELECT  OPTION  order_code
```

where

order_code is the order code (8 alphanumeric characters) assigned by Nortel

Record the textual name for the option shown under the NAME heading and then go to step 1.

Note: For assistance, contact the personnel responsible for the next level of support.

9 To stop processing of the ASSIGN STATE command, press the Enter key. The system response *Command cancelled*. indicates the command has been cancelled.

Go to step 1.

10 Check that you have entered the correct order code. If you have not, go to step 1.

Note: For assistance, contact the personnel responsible for the next level of support.

11 If the option is a state option, follow the procedure for assigning RTU in Chapter . If the option is a dual option, follow the procedure for assigning a usage limit in Chapter .

When you have completed the procedure, go to step 1.

12 Read the reasons for the validation errors in the error message. Follow the solutions suggested in the error message and then go to step 1.

Note: For assistance, contact the personnel responsible for the next level of support.

13 Exit the SOC directory by typing

```
>QUIT
```

8 Assigning a warning threshold to an option

Option warnings

An option's warning thresholds allow you to set a usage level at which software optionality control (SOC) creates a log (SOC800). The warning threshold is for your operating company's convenience. For example, an operating company may set a warning threshold to 90% of the purchased usage limit to alert the company that more resources should be purchased. This threshold can be either a percentage of a usage limit or an absolute number. A warning threshold, unlike the usage limit, is not password-controlled.

The following procedure describes how to assign a warning threshold to an option. SOC creates a SOC507 log if a warning threshold is successfully assigned to an option. It creates a SOC508 log if problems are encountered.

For more information on SOC logs, see Appendix B, “SOC Logs."

Assigning a warning threshold to an option

1 Access the SOC directory by typing

>SOC

See Table 8-1, “System response when accessing the SOC directory."

Table 8-1 (Sheet 1 of 2)

If the system response is	Do	Reason
System response when accessing the SOC directory		
`User count exceeded; SOC in use by <user>`	step 2	Only one SOC session at a time can be active. The user ID of the user running the other session is shown in the response.

Table 8-1 (Sheet 2 of 2)

If the system response is	Do	Reason
`SOC is already running`	step 3	Your CI session already has a SOC session running.
`SOC cannot be used while a dump is in progress. SOC not started`	step 4	SOC cannot start because the system is performing an image dump.
`The SOC prompt`	step 5	You have started a SOC session.
`Couldn't allocate SOC command directory...SOC not started`	step 14	SOC cannot allocate the SOC directory because the FuncGrp office has a resource problem.
`Couldn't allocate mailboxes...SOC not started`	step 14	SOC cannot allocate its mailboxes because the FuncGrp office has a resource problem.

2 See Table 8-2, “Steps to follow when 'User count exceeded' appears."

Table 8-2

If	then
Steps to follow when “User count exceeded" appears	
you are certain that no other SOC session is running	reset the usage counter for the SOC session. ***Note:*** For assistance, contact the personnel responsible for your next level of support.
another SOC session is running	wait for the other SOC session to terminate and then go to step 1.

3 Wait for the other SOC session to terminate and then go to step 1.

4 Wait for the image dump to complete and then go to step 1.

5 To assign a warning threshold to an option, enter the ASSIGN THRESHOLD command by typing

```
>ASSIGN THRESHOLD threshold thresh_type TO order_code
```

where

threshold is the new threshold value for the option (see notes)

thresh_type specifies whether the threshold is a number or a percentage (PERCENT or ABSOLUTE; ABSOLUTE is the default)

order_code is the order code (8 alphanumeric characters), assigned to the option by Nortel

Note 1: If the threshold type (thresh_typ) is PERCENT, the threshold must be a number between 0 and 100. If the threshold type is ABSOLUTE, the threshold must be a number between 0 and 999999.

Note 2: If the limit for the option is monitored and the threshold type is PERCENT, you must specify 100 in the threshold field.

Example input

```
>ASSIGN  THRESHOLD 90 PERCENT  TO  CTX00001
```

6 See Table 8-3, “System response to the ASSIGN THRESHOLD command."

Table 8-3 (Sheet 1 of 2)

If the system response is	Do	Reason
System response to the ASSIGN THRESHOLD command		
`Unknown order code`	step 14	SOC does not have a record of the specified order code.
`Cannot set threshold on state-only option`	step 14	You have tried to assign a usage threshold to a state option.
`Illegal order code <code>`	step 14	The string you entered is not a valid order code.

Table 8-3 (Sheet 2 of 2)

If the system response is	Do	Reason
`Illegal threshold`	step 14	You have typed an incorrect value for threshold. If the threshold type (thresh_typ) is PERCENT, the threshold must be a number between 0 and 100. If the threshold type is PERCENT and the limit is monitored, the threshold must be 100. If the threshold type is ABSOLUTE, the threshold must be a number between 0 and 999999.
`Usage warning threshold set to <threshold> for option <option> <Warnings>`	step 14	The usage warning threshold for the option has been set. SOC has updated the SOC database with the new threshold value. The response may contain a message stating that the new threshold is not reachable because it is above the hard usage limit of the option or that the current usage of the option already exceeds the new threshold.

7 Check that you have entered the correct order code; if you have not, go to step 14.

Note: For assistance, contact the personnel responsible for your next level of support.

8 Check that you have entered the correct threshold value and then go to step 14.

Note: For assistance, contact the personnel responsible for your next level of support.

9 Exit the SOC directory by typing

```
>QUIT
```

9 Creating a SOC report

Software optionality control (SOC) reports provide information about the SOC options in the operating company's product computing module load (PCL).

Types of SOC reports

You can request four types of reports about SOC options: brief, pack, verbose, and full. You can create a report for all options or a report for a subset of options.

Reports can be created for

- a specific option, by order code or by name
- all options with an order code or a name that contains a specified sub-string
- all options in a specific group
- all state-based options, including dual
- all options in a specified state
- all options with a specific right-to-use (RTU) setting
- all usage-based options, including dual options
- all options with a current usage over the warning threshold
- all options with a current usage of zero (0)
- all options with a current usage other than zero (0)
- all options

The procedure in this chapter provides instructions for requesting a SOC report.

Brief report

The brief report is the default report. It contains one line for each option, with the

- order code
- name

- RTU status
- state
- current usage
- usage limit
- units of usage
- date of the last change for the RTU setting or usage limit of that option

If there is an error in the status of an option, an in-service trouble (ISTB) status indicator appears in the report beside the affected option.

The brief report also indicates whether each option is

- tracked (TRAK)
- pending (PEND)
- usage, with a current usage over the warning threshold (>THR)
- usage, with a current usage over the limit (>LIM)
- usage, with a current usage over the maximum SOC can record (>MAX)

Note: If more than one of THR, LIM and MAX apply to the option, only one appears in the report. The order of priority from highest to lowest is MAX, LIM, and THR.

Figure Chapter 9, "Creating a SOC report," on page -1 Figure 9-1, "Chapter 9, "Creating a SOC report," on page -1MAP display example of a brief report for all options," on page 9-5 shows an example of a brief report for all options in a PCL, and Figure Chapter 9, "Creating a SOC report," on page -1 Figure 9-2, "Chapter 9, "Creating a SOC report," on page -1MAP display example of a brief report for a single option," on page 9-6 shows a brief report requested for one option.

Pack report

The pack report is a compressed version of the brief report for all options in a PCL. The pack report is periodically sent by the operating company to Nortel. For every state option, the pack report specifies the state option's order code, RTU status, current state, and the date of its last RTU change. For every usage option, the pack report specifies the usage option's order code, current usage, usage limit, high water mark, and the date of the last limit change. For dual options, both state and usage information is provided. Pending and tracked options are flagged as such. Figure Chapter 9, "Creating a SOC report," on page -1 Figure 9-5, "Chapter 9, "Creating a SOC report," on page -1MAP display example of a pack reportxx," on page 9-9 is an example of a pack report.

Verbose report

The verbose report contains the one-line option descriptions in the brief report. It also contains dependency information for state and dual options, feature usage counts for usage and dual options, and the high water mark and threshold for usage and dual options. Figure Chapter 9, "Creating a SOC report," on page -1 Figure 9-3, "Chapter 9, "Creating a SOC report," on page -1MAP display example of a verbose report," on page 9-7 and figure Chapter 9, "Creating a SOC report," on page -1 Figure 9-4, "Chapter 9, "Creating a SOC report," on page -1MAP display example of a verbose report for one usage option," on page 9-8 are examples of a verbose report.

Full report

In addition to the verbose report content, the full report contains the feature identifiers, feature names, feature states, and the last change dates for included features.

Report terminology

The following terms are used in the reports:

- GROUP is the 3- or 4-character functional group code.
- OPTION is the 8-character option order code.
- NAME is the 20-character name of the option (without the group code).
- RTU specifies the right-to-use state of the option, Y (YES) or N (NO).
- STATE specifies the state of the option, either IDLE, ON, ITO (idle-to-on) or OTI (on-to-idle).
- USAGE specifies the current usage of the option.
- LIMIT shows the usage limit of the option; an S follows a soft limit.
- UNITS specifies the unit of usage.
- LAST CHG for options is the date of the last RTU change or limit change.
- OPTIONS NEEDED lists the option order codes on which the option depends. NONE indicates that the option has no dependencies. NO INFO indicates the option is a pending option. SOC does not keep a record of dependencies for pending options.
- OPTIONS NOT PERMITTED lists the option order codes that cannot be in the ON state when this option is in the ON state. If the option can be in the ON state at the same time as any other option, NONE is specified. NO INFO means the option is a pending option.

- THRESHOLD specifies the usage warning threshold.
- HIGHWATER specifies the usage high water mark.

> ***Note:*** In the reports, dashes are used in fields that are not relevant to the option. For state options, for example, the usage, limit, and units fields are filled with dashes.

Figures Chapter 9, “Creating a SOC report,” on page -1 Figure 9-1, “Chapter 9, “Creating a SOC report,” on page -1MAP display example of a brief report for all options,” on page 9-5 to Chapter 9, “Creating a SOC report,” on page -1 Figure 9-5, “Chapter 9, “Creating a SOC report,” on page -1MAP display example of a pack reportxx,” on page 9-9 show examples of SOC reports.

Report examples

Figure 9-1 Chapter 9, “Creating a SOC report,” on page -1MAP display example of a brief report for all options

```
CLLI:OTWANOX14B2    SOC OPTION STATUS SUMMARY          DATE:95/09/30
PCL NAME:NA006

GROUP:SOC
OPTION      NAME            RTU STATE  USAGE  LIMIT   UNITS  LAST_CHG
------      ----            --- -----  -----  -----   -----  --------
SOCOPT10    Option 10       N/A IDLE       –      –       –  95/09/26
SOCOPT11    Option 11       A/P   ON       –      –       –  95/09/26
SOCOPT12    Option 12         Y    –       0    100 UNIT_12  95/09/26
SOCOPT13    Option 13         N IDLE       –      –       –  95/09/26
SOCOPT14    Option 14       N/A    –       0      0 UNIT_15  95/09/26
SOCOPT15    Option 15         N IDLE       0      0 UNIT_15  95/09/26
SOCOPT16    Option 16         N IDLE       –      0 UNIT_16  95/09/26 TRAK
```

Figure 9-2 Chapter 9, “Creating a SOC report,” on page -1MAP display example of a brief report for a single option

```
GROUP:ABS
OPTION      NAME                RTU STATE  USAGE  LIMIT  UNITS  LAST_CHG
------      ----                --- -----  -----  -----  -----  --------
ABS00008    TOPS Comm Cred Card   Y  IDLE      –      –      –  94/07/06
```

Figure 9-3 Chapter 9, “Creating a SOC report,” on page -1MAP display example of a verbose report

```
GROUP:ABC
OPTION   NAME                    RTU  STATE  USAGE  LIMIT  UNITS  LAST_CHG
------   ----                    ---  -----  -----  -----  -----  --------
ABCOPT17 Option 17                 N   IDLE      0      0  UNIT_AB 96/08/14
            options needed             NONE
            options not permitted      NONE
            threshold       75%        high water mark        0

            FEATURE   STATE   USAGE    UNITS
            -------   -----   -----    -----
            ABCFT170   IDLE   0        UNIT_AB
              NAME:   ABC Sample Usage Feature 0 with UNIT_AB
            ABCFT171   IDLE   0        UNIT_AB
              NAME:   ABC Sample Usage Feature 1 with UNIT_AB
            ABCFT172   IDLE   0        UNIT_AB
              NAME:   ABC Sample Usage Feature 2 with UNIT_AB
```

Figure 9-4 Chapter 9, “Creating a SOC report,” on page -1MAP display example of a verbose report for one usage option

```
GROUP:SOC
OPTION     NAME             RTU   STATE    USAGE  LIMIT   UNITS  LAST_CHG
------     ----             ---   -----    -----  -----   -----  --------
SOCOPT12   Option 12          Y       –       40    100 UNIT_12  95/03/14
           threshold:           90%  high water mark:       60
```

Figure 9-5 Chapter 9, “Creating a SOC report,” on page -1MAP display example of a pack reportxx

```
SOC OPTION STATUS SUMMARY
OTWAONXBDS0
TOPS03.1
940406
CTX00128 N I 930818
CTX00130 Y O 930508
CTX00131 Y I 931024
CTX00140 102 200 143 930523
CTX00141 203 200S 203 930523
CTX00173 N I 930508
OSDA0011 Y O 2342340 MONITORED
2342340 940101
OSDA0012 Y – 940404 TRAK
USDA0013 Y – 960606 PEND
USDA0014 – 200 – 931010 TRAK
USDA0015 Y – – 1000 – 931212 TRAK
0AFC24B1021845645AD4
```

Creating a SOC report

At the <location>

1 Access the SOC directory by typing

>SOC

See Table 9 9-1, System response when accessing the SOC directory.

Table 9-1

If the system response is	Do	Reason
9System response when accessing the SOC directory		
`User count exceeded; SOC in use by <user>`	step 2	Only one SOC session at a time can be active. The user ID of the user running the other session is shown in the response.
`SOC is already running`	step 3	The response means that your CI session already has a SOC session running.
`SOC cannot be used while a dump is in progress. SOC not started`	step 4	The response indicates that SOC cannot start because the system is performing an image dump.
`The SOC prompt`	step 23	You have started a SOC session.
`Couldn't allocate SOC command directory...SOC not started`	step 1	The response indicates that SOC cannot allocate the SOC directory because the FuncGrp office has a resource problem.
`Couldn't allocate mailboxes...SOC not started`	step 1	The response indicates that SOC cannot allocate its mailboxes because the FuncGrp office has a resource problem.

2 See Table 9 , “Steps to follow when “User count exceeded" appears."

Table 9-2

If	then
9Steps to follow when “User count exceeded" appears	
you are certain that no other SOC session is running	reset the usage counter for the SOC session. ***Note:*** For assistance, contact the personnel responsible for your next level of support.
another SOC session is running	wait for the other SOC session to terminate and then go to step 1.

3 Wait for the other SOC session to terminate and then go to step 1.

4 Wait for the image dump to complete and then go to step 1.

5 Your next step depends on whether you want a report about all options in your PCL or about specific options.

See Table 9 9-3, “Specifying what kind of SOC report you want."

Table 9-3

If you want a report about	Do
9Specifying what kind of SOC report you want	
a specific subset of options	step 1
all options	step 1

6 To request a report about a specific subset of options, enter the SELECT command by typing

```
>SELECT  select_type  value  report_type
```

where

select_type defines the criteria for selecting the option or set of options for display. The choices are OPTION, STATE, RTU, NAME, GROUP, or USAGE.

value is the value that corresponds to the select_type parameter (see notes)

report_type is the type of report (BRIEF or VERBOSE) This parameter is optional. The default is BRIEF. If the VERBOSE parameter is used, feature usage counts for usage and dual options are shown in the report.

See Table 9 9-4, “Select type options."

Table 9-4

If the select type is	you can enter
9Select type options	
OPTION	up to 8 characters. SOC creates a report for every option with an order code containing the character string you enter.
STATE	ON, IDLE, ERR, or ALL. ALL selects all state options.
RTU	either Y (YES) or N (NO).
NAME	up to 25 characters. SOC creates a report for every option with the character string you enter.
GROUP	a 3 or 4 character group.
USAGE	ALL, NONZERO, ZERO, or OVER_THRESHOLD. ALL selects all usage options, including dual. NONZERO selects options with usage values greater than 0. ZERO selects options with a current usage of zero (0). OVER_THRESHOLD selects options whose current usage exceeds its warning threshold.

Example input

```
>SELECT  STATE  ON
```

Go to step 1.

7 To request a report about all options, enter the SELECT command by typing

```
>SELECT  ALL  report_type
```

where

report_type is — is the type of report (BRIEF, VERBOSE, or PACK) BRIEF the default.

Example input

```
>SELECT  ALL  VERBOSE
```

Go to step 1.

8 See Table 9 9-5, “System response to the SELECT command."

Table 9-5

If the system response is	Do	Reason
9System response to the SELECT command		
`Target file exists. Replace?`	step 1	SOC found a file with the same name as the report file you requested with the SELECT ALL PACK command.
`Memory allocation failure while trying to create report. Report not created.`	step 1	The memory required to create the report could not be allocated. The FuncGrp office may have insufficient memory.
`Internal error accessing SOC database. Report not created.`	step 1	SOC has experienced an internal failure. An incomplete report may be created.
`No options match the selection criteria`	step 1	SOC could not find any options that match the selection criteria you requested. The report will not be created.
`Illegal order code <order code>`	step 1	The string you entered is not a valid order code.
`Packed report written to file <file> on device <device>`	step 1	The report you requested with the SELECT ALL PACK command was successfully created. The response indicates the file to which the report was written and the device that the file is on.
`No options in table; nothing to report`	step 1	There are no options in the table. A report will not be created.

9 To create the new report and delete the existing one, enter YES in response to the prompt. If you do not want to replace the old file with a new one, enter NO. If you enter NO, the report will not be created.

Go to step 1.

10 Wait until the office traffic levels are lower, try to create the report again and then go to step 1.

11 Check to see if any SWER logs have been created.

12 To enter the SELECT command with a different selection criteria, return to step 1.

13 Try the SELECT command with a correct order code or with a different selection criteria and then go to step 1.

14 Exit the SOC directory by typing

```
>QUIT
```

Note: For assistance, contact the personnel responsible for your next level of support.

10 Auditing the SOC database

You can request a software optionality control (SOC) database audit. The audit reports any inconsistencies in the SOC data structures. It also checks for any discrepancies between the state for an option recorded in the SOC database and the state for the option in the software.

The SOC system automatically performs this daily audit at the time specified in the SOC_AUDIT_SCHEDULE parameter in the SOCVAR table described in Chapter 11, “Defining SOC variables." The following procedure shows how to request an additional SOC audit, which is a SOC audit in addition to the regularly scheduled audit. SOC creates a SOC400 log when the audit is finished. For each error found during the audit, SOC creates a log in the range of SOC300 to SOC326. For conditions that are significant but are not errors, SOC creates a log in the range of SOC402 to SOC404.

Auditing the SOC database

1 Access the SOC directory by typing

>SOC

See Table 10-1, “System response when accessing the SOC directory. "

Table 10-1 (Sheet 1 of 2)

If the system response is	Do	Reason
System response when accessing the SOC directory		
`User count exceeded; SOC in use by <user>`	step 2	Only one SOC session at a time can be active. The user ID of the user running the other session is shown in the response.
Note: For assistance, contact the personnel responsible for the next level of support.		

Table 10-1 (Sheet 2 of 2)

If the system response is	Do	Reason
`SOC is already running`	step 3	The response means that your CI session already has a SOC session running.
`SOC cannot be used while a dump is in progress. SOC not started`	step 4	The response indicates that SOC cannot start because the system is performing an image dump.
`the SOC prompt`	step 37	You have started a SOC session.
`Couldn't allocate SOC command directory...SOC not started`	step 1	The response indicates that SOC cannot allocate the SOC directory because the FuncGrp office has a resource problem.
`Couldn't allocate mailboxes...SOC not started`	step 1	The response indicates that SOC cannot allocate its mailboxes because the FuncGrp office has a resource problem.
Note: For assistance, contact the personnel responsible for the next level of support.		

2 See Table 10-2, “Steps to follow when “User count exceeded" appears."

Table 10-2

If	then
Steps to follow when “User count exceeded" appears	
you are certain that no other SOC session is running	reset the usage counter for the SOC session. ***Note:*** For assistance, contact the personnel responsible for your next level of support.
another SOC session is running	wait for the other SOC session to terminate and then go to step 1.

3 Wait for the other SOC session to terminate and then go to step 1.

4 Wait for the image dump to complete and then go to step 1.

5 To request an audit of the SOC database, enter the DBAUDIT command by typing

```
>DBAUDIT
```

See Table 10-3, “System response to the DBAUDIT command."

Table 10-3

If the system response is	Do	Reason
System response to the DBAUDIT command		
`SOC audit completed. No errors found`	step 1	An audit was performed, and no inconsistencies in the SOC database were found.
`<trouble details> SOC audit completed <n> errors found`	step 1	Errors were discovered during the audit. ***Note:*** For assistance, contact the personnel responsible for the next level of support.

6 Exit the SOC directory by typing

```
>QUIT
```

11 Defining SOC variables

The SOCVAR table allows the operating company to change some software optionality control (SOC) variables. This chapter describes the fields in the SOC table.

Note: Nortel recommends that you use the default values in the SOCVAR table.

SOCVAR table

The following table contains the name of the fields in the SOCVAR table, the acceptable values for these fields and the default values.

Table 11-1 10-SOCVAR field descriptions

Field name	Value range	Default value
SOC_AUDIT_SCHEDULE	time of day	06:30
SOC_REPORT_DEVICE	vector up to 12 characters	SFDEV
SOC_RTU_FILE_DEVICE	vector up to 12 characters	ALL

SOC_AUDIT_SCHEDULE

The SOC_AUDIT_SCHEDULE field specifies the time of day when the audit begins. The default value starts the daily audit at 06:30.

SOC_REPORT_DEVICE

The SOC_REPORT_DEVICE field specifies the name of the device to which the SOC report created by the audit is sent. SFDEV is the default.

SOC_RTU_DEVICE

The SOC_RTU_DEVICE field specifies the name of the device from which the key code file is read. ALL is the default and specifies that all devices listed in table PADNDEV be searched. Device SFDEV is also searched whether or not it is listed in table PADNDEV.

Appendix A List of UCS DMS-250 SOCs

This appendix provides a comprehensive list of UCS DMS-250 Software Optionality Controls (SOCs). The SOCs are separated into the following sections:

- Billing and fraud SOCs
- Card services SOCs
- Carrier advanced intelligent network (CAIN) SOCs
- Dialable wideband services (DWS) SOC
- Dynamically-controlled routing (DCR) SOCs
- Engineering and administrative data acquisition (EADAS) SOC
- Gateway inter-machine trunk (IMT) SOC
- International trunk agents SOCs
- N00 routing SOCs
- Network interface-primary rate interface (PRI) SOC
- Network services SOCs
- Optional base SOC
- Programmable service node (PSN) SOC
- Release link trunk (RLT) SOCs
- Translations and routing SOCs

Table Table A-1, “,” on page A-2, “Finding a specific SOC order code," shows which SOCs each section contains. Each section contains a table. Inside the

table, the SOCs are listed alphabetically by order code. Beside each order code is the SOC's name and a brief description of the SOC.

Table A-1

SOC function	SOC order codes
Finding specific SOC order codes	
Billing and fraud SOCs	UBFR0001 through UBFR0005
Card services SOCs	CRDS0001 through CRDS0005
Carrier advanced intelligent network (CAIN) SOCs	CAIN0100, CAIN0200, CAIN0201, CAIN0300, CAIN0400, CAIN0500 through CAIN0513, CAIN0600 through CAIN0607, CAIN0609, CAIN0610, CAIN0700, CAIN0800 through CAIN0802, CAIN0900, CAIN0901
Dialable wideband service (DWS) SOC	UDWS0001
Dynamically-controlled routing SOCs	DCR00001 through DCR00004
Engineering and administrative data acquisition (EADAS) SOCs	OAM00004 through OAM00006, OAM00007, and OAM00010
Gateway inter-machine trunk (IMT) SOC	GIMT0003
International trunk agents SOCs	GIMT0001,GIMT0002, and GLR20001
N00 routing SOCs	N00R0001 through N00R003, and N00R0200
Network interface-primary rate interface (PRI) SOC	NPRI0001 and NPRI0002
Network services SOCs	NSER0001 through NSER0004 and NXXR001 through NXXR002
UCS base SOC	UCSB0001
Programmable service node (PSN) SOC	UPSN0001
Release link trunk (RLT) SOCs	PRLT0001, URLT0001 through URLT0004
Translations and routing SOCs	UTRS0001 through UTRS0005, UTRS0200 and UTRS0201

Billing and fraud SOCs

Table Table A-2, “,” on page A-3, “Billing and fraud SOCs," provides a comprehensive list of the billing and fraud SOCs.

Table A-2 (Sheet 1 of 2)

Order Code	Name	Description
Billing and fraud SOCs		
UBFR0001	0 Flexible CDR	UBFR0001 provides the ability to define and use different call detail record (CDR) formats for each-trunk group or for each-subscriber number basis. ***Note:*** For more information on UBFR0001, see the *UCS-DMS-250 Billing Records Appilcation Guide*.
UBFR0003	0 Fraud Enhancements	UBFR0003 provides the ability to control two functions: • Limited Calls for each Authcode—allow only a selected number of active calls for each authcode and block any other call attempts with the same authcode. • Enhanced Network Security (NETSEC)—provides Network Security profile screening to the NETSEC functionality. ***Note:*** For more information on UBFR0003, see the *UCS DMS-250 Feature Group D Application Guide*.
UBFR0004	0 MCCS Fraud Enh	UBFR0004 provides the ability for ANI (Automatic Number Identification) screening for UA (Universal Access) MCCS (Mechanized Calling Card Services) calls on FGD (Feature Group D) trunks. ***Note:*** For more information on UBFR0004, see the *UCS DMS-250 Mechanized Calling Card Services (MCCS) Application Guide*.

Table A-2 (Sheet 2 of 2)

Order Code	Name	Description
UBFR0005	0 Auto CDR Throttlin	UBFR0005 provides the ability for automatically throttling the CDRs for calls on SS7 Intra IMT originators to aid in diminishing the loss of CDR data for billable calls during a very high percentage of recording units in use. Alternatively, it may be used to reduce the amount of CPU time spent in collecting and formatting billing data during busy periods, in order to provide increased call handling capacity. ***Note:*** For more information on UBFR0005, see the *UCS DMS-250 Billing Records Application Guide*.
UBFR0005	0 Auto CDR Throttlin	UBFR0005 provides the ability for automatically throttling the CDRs for calls on SS7 Intra IMT originators to aid in diminishing the loss of CDR data for billable calls during a very high percentage of recording units in use. Alternatively, it may be used to reduce the amount of CPU time spent in collecting and formatting billing data during busy periods, in order to provide increased call handling capacity. ***Note:*** For more information on UBFR0005, see the *UCS DMS-250 Billing Records Application Guide*.
UBFR0006	0 Long Call Fraud Delection	When UBFR006 is in the ON state it provides the ability to run the long call audit more frequently than once every 24 hours with the possible option of disconnecting the long call. If UBFR006 is in IDLE state, none of the enhanced features for the long call audit are accessible. However, table LCAUDIT can still be datafilled but the information stored in that table is not screened by the long call audit. UBFR006 in IDLE state indicates the original long call audit functionalities are used. ***Note:*** For more information on UBFR0006, see the *UCS DMS-250 Billing Records Application Guide*.

Card services SOCs

Table Table A-3, “,” on page A-5, “Card services SOCs," provides a comprehensive list of UCS DMS-250 card services SOCs.

Table A-3 (Sheet 1 of 3)

Order Code	Name	Description
Card services SOCs		
CRDS0001	Card Services	CRDS0001 provides basic 14-digit travel card services on the UCS DMS-250 system: • Calling Card allows service providers to offer calling card services, so subscribers can place calls through the UCS DMS-250 system from any location and have the billing charged against a 14-digit calling card. • Enhanced Calling Card allows COSUS access to block or allow international and direct dial calls for each calling card basis. • Travel Card Number (TCN) Log Enhancements provides the service provider with a log after each failed attempt to enter a valid 14-digit TCN. • Mechanized Calling Card Services (MCCS) Dedicated supports travel card number calling with or without the 0 prefix in the called address for national calls. ***Note:*** For more information on CRDS0001 see the *UCS DMS-250 Mechanized Calling Card Services Application Guide.*

Table A-3 (Sheet 2 of 3)

Order Code	Name	Description
CRDS0002	TCAP Card Services	CRDS0002 provides TCAP-based travel card number and CI Command TESTSS (or ACCTTEST) for TCN validation: • TCAP-Based TCN allows the service provider to support calling card services with an off-board SCP to validate the calling card. • CI Command TESTSS (ACCTTEST) enables queries to be sent to an SCP and displays the results. ***Note 1:*** You must have SOC CRDS0001 to use SOC CRDS0002. ***Note 2:*** For more information on CRDS0002 see the *UCS DMS-250 Mechanized Calling Card Services (MCCS) Application Guide.*
CRDS0003	MVP Card Services	CRDS0003 allows service providers to use Mechanized Voice Prompts (MVPs) instead of tone-based prompts. ***Note 1:*** You must have SOC CRDS0001 to use SOC CRDS0003. ***Note 2:*** For more information on CRDS0003 see the *UCS DMS-250 Mechanized Calling Card Services (MCCS) Application Guide.*

Table A-3 (Sheet 3 of 3)

Order Code	Name	Description
CRDS0004	CLG/CLD Number Query	CRDS0004 adds two digits parameters to the IN1 MCCS TCAP INVOKE message, the Calling (CLG) Party Address Digits Parameter and the Called (CLD) Party Address Digits Parameter. To use this feature the office parm ENHANCED_TCN_TCAP must be turned ON. ***Note:*** This fold-in feature does not change the IN1 MCCS TCAP RETURN RESULT message; only the INVOKE message is modified.
CRDS0005	Quick Call	CRDS0005 allows subscribers who are calling their home to dial a four-digit number instead of their full travel card number (TCN). ***Note 1:*** You must have SOC CRDS0001 to use SOC CRDS0005. ***Note 2:*** For more information on CRDS0005 see the *UCS DMS-250 Mechanized Calling Card Services (MCCS) Application Guide.*

Carrier advanced intelligent network (CAIN) SOCs

Table Table A-4, “,” on page A-7, “Carrier advanced intelligent network (CAIN) SOCs," provides a comprehensive list of UCS DMS-250 CAIN SOCs.

Table A-4 (Sheet 1 of 9)

Order Code	Name	Description
Carrier advanced intelligent network (CAIN) SOCs		
CAIN0100	Messages	CAIN0100 enables service providers to purchase a specified number of carrier advanced intelligent CAIN messages, which helps service providers make a more gradual investment in Carrier AIN. ***Note 1:*** CAIN0100 can be licensed separately from other CAIN ordering codes. ***Note 2:*** For more information on CAIN0100, see the *UCS DMS-250 NetworkBuilder Application Guide.*

Table A-4 (Sheet 2 of 9)

Order Code	Name	Description
CAIN0200	Extension Parms	CAIN0200 supports an extended parameter set on the UCS DMS-250 system service switching point (SSP) AIN 0.2 to convey optional, feature-specific information that the standard AIN 0.2 parameter set may have trouble transmitting. Particularly, CAIN0200 allows you to route each plain old telephone service (POTS) termination through separate serving translations schemes (STS), which allows you to provide a more diverse range of terminating options. ***Note 1:*** CAIN0200 can be licensed separately from other CAIN ordering codes. ***Note 2:*** For more information on CAIN0200, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0300	SCP Simulator	CAIN0300 allows the service control point (SCP) simulator to interface with the UCS DMS-250 platform's implementation of AIN 0.2. The SSP uses the SCP simulator to test AIN 0.2 functionality. ***Note 1:*** CAIN0300 can be licensed separately from other CAIN ordering codes. ***Note 2:*** For more information on CAIN0300, see the UCS DMS-250 NetworkBuilder Application Guide.
CAIN0400	Test Query Tool	CAIN0400 provides the capability to initiate test messages to an SCP and to receive its responses. ***Note 1:*** CAIN0400 can be licensed separately from other CAIN ordering codes. ***Note 2:*** For more information on CAIN0400, see the UCS DMS-250 NetworkBuilder Application Guide.
CAIN0500	CUSTDP Trigger	CAIN0500 supports the Customized_Dialing_Plan (CUSTDP) trigger, which is used to implement Virtual Private Network (VPN) services. ***Note 1:*** CAIN0500 can be licensed separately from other CAIN ordering codes. ***Note 2:*** For more information on CAIN0500, see the UCS DMS-250 NetworkBuilder Application Guide.

Table A-4 (Sheet 3 of 9)

Order Code	Name	Description
CAIN0501	SPECDIG Trigger	CAIN0501 supports the Specific_Digit_String (SPECDIG) trigger, which is used to implement 800/N00 services, as well as off-board ANI screening. ***Note 1:*** CAIN0501 can be licensed separately from other CAIN ordering codes. ***Note 2:*** For more information on CAIN0501, see the UCS DMS-250 NetworkBuilder Application Guide.
CAIN0502	OFFHKIM Trigger	CAIN0502 supports the Off_Hook_Immediate (OFFHKIM) trigger which implements services that use nonstandard dialing plans, such as the following four services: • Speed dialing • Hotline • Menu routing • Military dialing ***Note 1:*** CAIN0502 can be licensed separately from other CAIN ordering codes. ***Note 2:*** For more information on CAIN0502, see the UCS DMS-250 NetworkBuilder Application Guide.
CAIN0503	SIOTRK Trigger	CAIN0503 supports the Shared_Interoffice_trunk (SIOTRK) trigger which is used to support the following services: • Authcode/Account Code/PIN Screening • 500 - Find Me • CIC Routing • ANI Screening ***Note 1:*** CAIN0503 can be licensed separately from other CAIN ordering codes. ***Note 2:*** For more information on CAIN0503, see the UCS DMS-250 NetworkBuilder Application Guide.

Table A-4 (Sheet 4 of 9)

Order Code	Name	Description
CAIN0504	PRIBCHNL Trigger	CAIN0504 supports the PRI_B_Channel (PRIBCHNL) trigger which implements the following three services: • Dial 1 + • N00 • Subscriber screening ***Note 1:*** CAIN0504 can be licensed separately from other CAIN ordering codes. ***Note 2:*** For more information on CAIN0504, see the UCS DMS-250 NetworkBuilder Application Guide.
CAIN0505	ONOANSWER Trigger	CAIN0505 supports the O_No_Answer (ONOANSWER) trigger which allows subscribers to specify a time interval during which the called party should answer a call. It provides busy services such as the following three services: • Call Redirect • Call Take Back • Message Delivery for 800 subscribers ***Note 1:*** CAIN0505 can be licensed separately from other CAIN ordering codes. ***Note 2:*** For more information on CAIN0505, see the UCS DMS-250 NetworkBuilder Application Guide.
CAIN0506	NETBUSY Trigger	CAIN0506 implements the Network_Busy (NETBUSY) trigger which implements the following services when network congestion occurs: • Network forwarding • Network queuing • Network rerouting Network Rerouting services. Network Busy occurs in two scenarios: ***Note:*** For more information on CAIN0506 see the UCS DMS-250 NetworkBuilder Application Guide.

Table A-4 (Sheet 5 of 9)

Order Code	Name	Description
CAIN0507	OCLDBUSY Trigger	CAIN0507 implements the O_Called_Party_Busy (OCLDBUSY) trigger which implements the following services: • Call Forwarding • Rerouting on Busy Signal ***Note:*** For more information on CAIN0507, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0508	OFTRREQ Trigger	CAIN0508 implements the O_Feature_Requested (OFTRREQ) trigger which implements the following services: • Dial 1+ • Enhanced Travel Card • Universal Access for Authorization Codes ***Note:*** For more information on CAIN0508, see the UCS DMS-250 NetworkBuilder Application Guide.
CAIN0509	OIECREO Trigger	CAIN0509 implements the O_IEC_Reorigination (OIECREO) trigger which controls and provides enhanced reorigination services. ***Note:*** For more information on CAIN0509, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0510	TERMATT Trigger	CAIN0510 implements the Termination_Attempt (TERMATT) trigger, which implements caller ID delivery services. ***Note:*** For more information on CAIN0510, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0511	SPECFEAT Trigger	CAIN0511 implements the Specific_Feature_Code (SPECFEAT) trigger. ***Note:*** For more information on CAIN0511, see the *UCS DMS-250 NetworkBuilder Application Guide.*

Table A-4 (Sheet 6 of 9)

Order Code	Name	Description
CAIN0512	OFFHKDEL Trigger	CAIN0512 implements the Off-hook_Delay (OFFHKDEL) trigger, which allows the UCS DMS-250 switch to interrupt the dial plan and query the SCP when the UCS DMS-250 switch has collected the initial set of address digits. ***Note:*** For more information on CAIN0512, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0513	TOLLFREE Trigger	CAIN0513 allows the ability to subscribe to multiple CAIN groups, which allows for a service integration of the IN/1 trigger offerings (TOLLFREE) and the CAIN triggers. TOLLFREE trigger evaluation occurs between the O_Feature_Requested and Off_Hook_Delay CAIN triggers. ***Note:*** For more information on CAIN0513, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0600	Con Digit Collect	CAIN0600 allows the SCP to do prompted digit collection [Con Digit Collect (Conversational Digit Collection)] using the Send_to_Resource message. It allows operating companies to construct more flexible dialing plans. ***Note:*** For more information on CAIN0600 see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0601	SCP Trigger Sub	CAIN0601 enables the SCP to send the CAINGRP extension parameter that specifies a group of triggers that are checked later in the call model. ***Note:*** For more information on CAIN0601, see the *UCS DMS-250 NetworkBuilder Application Guide.*

Table A-4 (Sheet 7 of 9)

Order Code	Name	Description
CAIN0602	EDPs	CAIN0602 supports the following EDPs (Event Detection Points): • O_Called_Party_Busy • O_No_Answer • O_Term_Seized • O_Answer • Network_Busy ***Note:*** For more information on CAIN0602, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0603	STR Connection	CAIN0603 allows a connection with an intelligent peripheral (IP) to be initiated by using the Send_To_Resource message. ***Note:*** For more information on CAIN0603, see the UCS DMS-250 NetworkBuilder Application Guide.
CAIN0604	Inter IMT Support	CAIN0604 allows SS7 Global inter-machine trunks (IMT) to invoke CAIN triggers. ***Note:*** For more information on CAIN0604, see the UCS DMS-250 NetworkBuilder Application Guide.
CAIN0605	Global IMT Support	CAIN0605 allows SS7 Global IMT trunks to invoke CAIN triggers. ***Note:*** For more information on CAIN0605, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0606	1129-Style IP	CAIN0606 supports the exchange of data when connecting to an intelligent peripheral (IP), as specified by GR-1129 CORE (Switch-Intelligent Peripheral Interface) ***Note:*** For more information on CAIN0606, see the *UCS DMS-250 NetworkBuilder Application Guide.*

Table A-4 (Sheet 8 of 9)

Order Code	Name	Description
CAIN0607	Virtual IP	CAIN0607 enables the service control point (SCP) to control the in-switch dialing plan based on the information contained in the Flex Parameter Block sent in Send_To_Resource messages. ***Note:*** For more information on CAIN0607, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0609	Term Notification	CAIN0609 provides NetworkBuilder support for the “Termination Notification" event based upon Bellcore AIN 0.2 requirements GR-1298 and GR-1299. ***Note:*** For more information on CAIN0609, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0610	CainPrt Digit Coll	CAIN0610 allows the use of CainPrt table and O_Feature_Requested trigger. ***Note:*** For more information on CAIN0610, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0700	LNP Q00	CAIN0700 implements local number portability (LNP) query-on origination (QOO), which allows subscribers to retain their directory numbers when they change service providers. CAIN0700 controls the LNP function, OFFCCODE trigger table lookup and querying. ***Note:*** For more information on CAIN0700, see the *UCS DMS-250 Local Number Portability Application Guide.*
CAIN0800	Mid Call Services 1	CAIN0800 supports the following EDPs: • O_Mid_Call • O_Disconnect ***Note:*** For more information on CAIN0800, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0801	Mid Call Services 2	CAIN0801 controls whether or not the SSP is allowed to process a CTR message received from the SCP at the Timeout event. ***Note:*** For more information on CAIN0801, see the *UCS DMS-250 NetworkBuilder Application Guide.*

Table A-4 (Sheet 9 of 9)

Order Code	Name	Description
CAIN0802	Takeback & Transfer	CAIN0802 supports the switchHookFlash event at the O_Mid_Call EDP.
CAIN0900	Auto Code Gapping	CAIN0900 provides SCP Override automatic code gapping (ACG) control. ***Note:*** For more information on CAIN0900, see the *UCS DMS-250 NetworkBuilder Application Guide.*
CAIN0901	Manual Code Gapping	CAIN0901 provides SOCC ACG control. ***Note:*** For more information on CAIN0901, see the *UCS DMS-250 NetworkBuilder Application Guide.*

Dialable wideband services (DWS) SOC

Table Table A-5, “,” on page A-15, “Dialable wideband services (DWS) SOC," describes the DWS SOC.

Table A-5

Order Code	Name	Description
Dialable wideband services (DWS) SOC		
UDWS0001	UCS Dialable Widebnd	UDWS0001 provides long-distance applications with Dialable Wideband Services (DWS): • DWS FGD ISUP provides bandwidth-on- demand services over SS7 Feature Group D (FGD) trunks. • DWS IMT ISUP provides bandwidth-on-demand services for CCS7 ISDN User Part (ISUP) inter-machine trunks (IMTs), which allows DWS traffic to go through the service provider's UCS DMS-250 network. • DWS PRI allows the service provider to offer DWS service to subscribers who require direct PRI terminations. It also allows ISUP DWS to work with PRI DWS for end-to-end connectivity. ***Note:*** For more information on UDWS0001 see the *UCS DMS-250 Dialable Wideband Services Application Guide.*

Dynamically-controlled routing (DCR) SOCs

Table Table A-6, “,” on page A-16, “Dynamically-controlled routing (DCR) SOCs," provides a comprehensive list of UCS DMS-250 DCR SOCs.

Table A-6 (Sheet 1 of 2)

Order Code	Name	Description
Dynamically-controlled routing (DCR) SOCs		
DCR00001	DCR	DCR00001 provides dynamically-controlled routing (DCR) of overflow traffic. ***Note:*** For more information on DCR00001, see the *DMS-100 DCR User Guide.*
DCR00002	Mult. Net. Access	DCR00002 allows the switch to send calls to another network by means of gateway switches that are part of both networks. ***Note 1:*** DCR00002 is an order code and not a SOC. ***Note 2:*** For more information on DCR00002, see the *DMS-100 DCR User Guide.*

Table A-6 (Sheet 2 of 2)

Order Code	Name	Description
DCR00003	Dual X25 link	DCR00003 allows the Network Processor (NP), a centralized processor that communicates with DCR switches, to establish a backup communication facility for DCR messages between the UCS DMS-250 switch and the NP for all active DCR networks. ***Note 1:*** You must have SOC DCR00001 to use SOC DCR00003. ***Note 2:*** For more information on DCR00003, see the *DMS-100 DCR User Guide.*
DCR00004	Univrsal Translation	DCR00004 supports DCR selectors in the seven universal translation routing tables: • ACRTE • CTRTE • FARTE • FTRTE • NSCRTE • OFCRTE • PXRTE ***Note 1:*** You must have SOC DCR00001 to use SOC DCR00004. ***Note 2:*** For more information on DCR00004 see the *DMS-100 DCR User Guide.*

Engineering and administrative data acquisition (EADAS) SOCs

Table Table A-7, “,” on page A-18, “Engineering and administrative data acquisition (EADAS) SOCs," provides a comprehensive list of the EADAS SOCs.

Table A-7 (Sheet 1 of 2)

Order Code	Name	Description
Engineering and administrative data acquisition (EADAS) SOCs		
OAM00004	EADAS Data Collection Interface	OAM00004 provides protocol conversion and data link capabilities enabling operational measurements (OMs) stored in the UCS DMS-250 switch to be issued by EADAS-compliant Operational Support Systems. OAM00004 supports TR-740 compliancy and the transmission of UCS DMS-250 OMs.
OAM00005	EADAS Network Management Interface	OAM00005 allows EADAS-compliant Operational Support Systems (OSS) to provide surveillance, rerouting, reporting, traffic load monitoring, and control capabilities in the UCS DMS-250 switch. OAM00005 also provides traffic management OM data to the EADAS/Network Management (NM) Center and processes audit and control messages received from the EADAS/NM Center. It supports Bellcore TR-746 compliant header and byte order transmission. ***Note 1:*** You must have SOC OAM00004 to use OAM00005 . ***Note 2:*** Do not use SOC UOAM0002 with SOC UOAM0003.

Table A-7 (Sheet 2 of 2)

Order Code	Name	Description
OAM00006	Enhanced Network Management Interface	OAM00006 allows EADAS-compliant Operational Support Systems (OSSs) to provide surveillance, rerouting, reporting, traffic load monitoring, and control capabilities in the UCS DMS-250 switch. OAM00006 provides an enhanced network management interface based on Bellcore's proprietary SR-3942 specification. This interface can transmit traffic measurement OMs for up to 1024 trunk groups to be processed by network management processing systems. It also supports audit and control messages to the UCS DMS-250 switch. ***Note 1:*** You must have SOC OAM00004 to use SOC OAM00006. ***Note 2:*** Do not use SOC OAM00006 with SOC OAM00005.
OAM00007	Expanded Buffer Size	OAM00007 increases the EADAS buffer size from 32K to 256K. ***Note:*** You must have SOC OAM00004 to use SOC OAM00007.
OAM00010	EADAS MTC Bsy Usage	OAM00010 provides the Trunk Maintenance Busy Usage counts which is of paramount importance for the proper surveillance of the telephone network.

Gateway inter-machine trunk (IMT) SOC

Table Table A-8, “,” on page A-20, “Gateway inter-machine trunk (IMT) SOC," describes the Gateway IMT SOC.

Table A-8

Order Code	Name	Description
Gateway inter-machine trunk (IMT) SOC		
GIMT0003	0 UCS250 Gateway	GIMT0003 allows Global IMT trunks to function as gateway trunks between a UCS DMS-250 switch and a foreign exchange in the international network. ***Note 1:*** GIMT0003 does not depend on SOCs GIMT0001 and GIMT0002. ***Note 2:*** For more information on GIMT0003, see the *UCS DMS-250 Gateway IMT Application Guide*

International trunk agents SOCs

Table Table A-9, “,” on page A-20, “International trunk agents SOCs," provides a comprehensive list of UCS DMS-250 international trunk agents SOCs.

Table A-9 (Sheet 1 of 2)

Order Code	Name	Description
International trunk agents SOCs		
GIMT0001	Open Number Plan	GIMT0001 places the DMS-250 in the non-World Zone-1 market. It supports, on calls originating from ITU Global IMTs and Mexican Global IMTs, call routing and translation based on the CIC (Carrier Identification Code) in the Incoming Address Message (IAM) or the dialed digits. It also provides Flexible Service Access Calls (FSAC) on ITU IMTs and Mexican IMTs. FSAC calls are also known as free phone and premium services. They correspond to the N00 functionality in the World Zone-1 market. When GIMT0001 is ON, the market is assumed to be outside World Zone-1. ***Note:*** For more information on GIMT0001, see the *UCS DMS-250 International Application Guide.*

Table A-9 (Sheet 2 of 2)

Order Code	Name	Description
GIMT0002	Mexican ISUP	GIMT0002 implements the Mexican ISUP protocol on the UCS DMS-250 switch to make the UCS DMS-250 switch compliant in the Mexican market: • GIMT0002 allows Mexican ISUP signaling to support calls originating and terminating on the Mexican ISUP IMT (Global) trunk. • GIMT0002 provides interworking between Mexican ISUP IMT (Global) trunk and UCP ISUP IMT (Intra and Global) trunk, Mexican ISUP IMT (Global) trunk, and Mexican R2 trunk. ***Note 1:*** You must have SOC GIMT0001 to use SOC GIMT0002. ***Note 2:*** For more information on GIMT0002, see the *UCS DMS-250 International Application Guide.*
GLR20001	Global R2	GLR20001 enables Mexican R2 trunks on the UCS DMS-250 switch. ***Note 1:*** You must have SOC GIMT0001 to use SOC GLR20001. ***Note 2:*** For more information on GLR20001, see the *UCS DMS-250 International Application Guide.*

N00/NXX routing SOCs

Table Table A-10, “,” on page A-22, “N00/NXX routing SOCs," provides a comprehensive list of UCS DMS-250 N00/NXX routing SOCs.

Table A-10 (Sheet 1 of 4)

Order Code	Name	Description
N00/NXX routing SOCs		
N00R0001	N00 Routing	N00R0001 provides basic N00 routing services and Info Digit 24 functionality: • N00 Routing allows service providers who opt to process N00 calls without using an SCP to provide N00 routing services using UCS DMS-250 switch system datafill. • Info Digit 24 Functionality enables the service provider to recognize 10-digit received numbers as having originally been 800 numbers that have been translated to the actual destination address. ***Note:*** For more information on N00R0001, see the *UCS DMS-250 International Application Guide.*

Table A-10 (Sheet 2 of 4)

Order Code	Name	Description
N00R0002	N00/NXX TCAP SERVICE	N00R0002 provides TCAP-based N00 Routing: • TCAP-based N00 Routing provides N00 routing services for subscribers by using a centralized Service Control Point (SCP) to translate the dialed N00 number. Using the TCAP protocol provided by CCS7 signaling, the UCS DMS-250 platform routes caller and N00 number information to an SCP for lookup. • TCAP-based NXX Dialing Plan enables service providers to offer additional toll-free numbers and emerging toll-free services. • Auto Code Gapping (ACG) allows the UCS DMS-250 switch to prioritize TCAP query messages, upon request from the SCP, based upon predefined priority levels. • Auto Code Gapping Command Increment (ACGCI) command allows you to control the ACG through the CI. ***Note:*** For more information on the ACGCI command, see the *UCS DMS-250 Commands Reference Manual.* • N00 TCAP Route Advance allows the UCS DMS-250 switch to re-route an N00 call to predefined alternative destinations. ***Note:*** For more information on N00R0002, see the *UCS DMS-250 Transaction Capabilities Application Part (TCAP) Application Guide*

Table A-10 (Sheet 3 of 4)

Order Code	Name	Description
N00R0003	V2 TCAP DNIS Svc	N00R0003 provides TCAP-based N00 Routing: • TCAP-based N00 Routing provides N00 routing services for subscribers by using a centralized Service Control Point (SCP) to translate the dialed N00 number. Using the TCAP protocol provided by CCS7 signaling, the UCS DMS-250 platform routes caller and N00 number information to an SCP for lookup. • TCAP-based NXX Dialing Plan enables service providers to offer additional toll-free numbers and emerging toll-free services. • Auto Code Gapping (ACG) allows the UCS DMS-250 switch to prioritize TCAP query messages, upon request from the SCP, based upon predefined priority levels. • Auto Code Gapping Command Increment (ACGCI) command allows you to control the ACG through the CI. ***Note:*** For more information on the ACGCI command, see the *UCS DMS-250 Commands Reference Manual.* • N00 TCAP Route Advance allows the UCS DMS-250 switch to re-route an N00 call to predefined alternative destinations. ***Note:*** For more information on N00R0003, see the *UCS DMS-250 Transaction Capabilities Application Part (TCAP) Application Guide*
N00R0200	UIFN	N00R0200 allows you to provide toll-free capabilities for international 800 numbers.
NXXR0001	NXX Blocking	NXXR0001 provides an in-switch capability to optionally block NXX calls based on the Information digits (Infodigs) received. ***Note:*** For more information on NXXR0001, see the *UCS DMS-250 International Application Guide.*

Table A-10 (Sheet 4 of 4)

Order Code	Name	Description
NXXR0002	Toll Free NXX Acct	NXXR0002 provides in-switch NXX Account Code validation functionality. ***Note:*** For more information on NXXR0002, see the *UCS DMS-250 International Application Guide.*
NXXR0003	DNIS Trunk Option	NXXR0003 provides control via datafill in Table TRKGRP for the Dialed Number Inward Services (DNIS) on N00/NXX calls to be forwarded through the Network to the terminator.

Network interface-primary rate interface (PRI) SOC

Table Table A-11, “,” on page A-25, “Network interface-primary rate interface (PRI) SOC," describes the network interface-PRI SOC.

Table A-11 (Sheet 1 of 2)

Order Code	Name	Description
Network interface-primary rate interface (PRI) SOC		
NPRI0001	PRI Netwk Interface	NPRI0001 provides primary rate interface (PRI) signaling features : • Access Transport provides six features: — ability to datafill PRI optional information elements into an ISUP ATP — interworking between PRI and ISUP when ATP is in operation — transport of Q.931 optional information elements across a UCS DMS-250 ISUP network in the ATP — method A name display — locking shift to extension codesets 5, 6, or 7

Table A-11 (Sheet 2 of 2)

Order Code	Name	Description
		transport of the following Q.931 optional information elements: • Higher Layer Compatibility (HLC) • Called Party Subaddress (CDS) • Calling Party Subaddress (CGS) PRI D-Channel Backup provides a back-up D-Channel to increase reliability and to guarantee continued PRI service between any switching nodes or networks that are using ISDN PRI. ***Note:*** For more information on NPRI0001, see the *DMS-100 Family Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) Maintenance Guide.*
NPRI0002	PRI II Digs	NPRI0002 allows outpulsing of Originating Line Information (OLI) or Information digits (II) on terminating primary rate interface (PRI) while utilizing the Nonstandard (N) Route selector to facilitate called party number digit manipulation. ***Note:*** For more information on NPRI0002, see the *DMS-100 Family Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) Maintenance Guide.*

Network services SOCs

Table Table A-12, “,” on page A-27, “Network services SOCs," provides a comprehensive list of the network services SOCs.

Table A-12 (Sheet 1 of 2)

Order Code	Name	Description
Network services SOCs		
NSER0001	Network Services	NSER0001 provides various network-level services that can be combined: • ANI Delivery on DALTIE provides real-time calling number delivery on Dedicated Access Line (DAL) Terminal Interface Equipment (TIE) trunks terminating from the UCS DMS-250 switch. • STS/Netinfo Mapping provides ISUP connectivity between a UCS DMS-250 switch using IMT trunks and a Nortel SL-100 using IBN7 trunks. The NETINFO parameter of the initial address message (IAM) exchanges the necessary translation information for each call. ***Note:*** For more information on NSER0001, see the *UCS DMS-250 International Application Guide*

Table A-12 (Sheet 2 of 2)

Order Code	Name	Description
NSER0002	TCAP Auth & Acct Val	NSER0002 uses an SCP to offer account code, speed dial, and authorization code validation services: • TCAP-Based Account Code and Private Speed Validation enables the service provider to offer account code and speed dial number services for subscribers using an off-board service control point (SCP) to verify the account code, translate the speed dial number, or both. • TCAP-Based Authorization Code Validation enables the service provider to offer authorization code services for their subscribers using an off-board SCP to verify the authorization code. ***Note:*** For more information on NSER0002, see the *UCS DMS-250 Transction Capabilties Application Part (TCAP) Application Guide*
NSER0003	Inter/Intra IMT	NSER0003 allows inter-machine trunks (IMTs) to be designated as either inter- or intra-network. It also provides IMT connectivity to the DSC DEX switch and supports universal access calls and reorigination on inter-network ISUP IMTs. ***Note:*** You must have SOC NSER0001 to use SOC NSER0003.

Optional base SOC

Table Table A-13, “,” on page A-29, “Optional base SOC," describes the optional base SOC.

Table A-13

Order Code	Name	Description
Optional base SOC		
UCSB0001	UCS Base	UCSB0001 provides the following optional long-distance features: • Class of Service Administration Enhancements • Expansion of Speed Dialing Indices • Cause and Treatment Mapping Enhancements • Carrier Selection Parameter CDR Enhancements • CDR Enhancements • Operator Routing Enhancements
Note: UCSB0001 is the order code for the UCS Base software and is not a SOC.		

Programmable service node (PSN) SOC

Table Table A-14, “,” on page A-30, “Programmable service node (PSN) SOC," describes the PSN SOC.

Table A-14

Order Code	Name	Description
Programmable service node (PSN) SOC		
UPSN0001	0 Prog Service Node	UPSN0001 provides a programmable switching matrix within the UCS DMS-250 switch. The PSN is controlled by an external Service control Unit (SCU) which is connected to the UCS DMS-250 switch by means of an Ethernet link. NetworkBuilder triggers are used to send calls from the UCS DMS-250 switch to the programmable service node (PSN) environment. In this environment, the SCU controls calls because it contains the service logic for enhanced services such as debit card, or international call back.

Release link trunk (RLT) SOCs

Table Table A-15, “,” on page A-30, “Release link trunk (RLT) SOCs," provides a comprehensive list of the RLT SOCs.

Table A-15 (Sheet 1 of 3)

Order Code	Name	Description
Release link trunk (RLT) SOCs		
PRLT0001	ISDN PRI RLT	PRLT0001 reduces port and trunking requirements by introducing Release Link Trunk (RLT) efficiencies. Integrated services digital network (ISDN) Primary Rate Interface (PRI) Release Link Trunk (RLT) allows service providers to optimize trunking facility by releasing PRI after call redirection. RLT significantly reduces holding times, which reduces the port requirements between the UCS DMS-250 switch and IP/PBX. ***Note:*** For more information on PRLT0001, see the *UCS DMS-250 PRI RLT Application Guide*.

Table A-15 (Sheet 2 of 3)

Order Code	Name	Description
URLT0001	0 SS7 RLT Base	URLT0001 provides three services: • Enhanced operator position system (EOPS) call sequencing provides reorigination for calling card, credit card, ANI, or authcode station-to-station or person-to-person, non-collect billed calls that terminate from EOPS. Reorigination enables a caller using a calling card to make multiple calls without redialing the carrier access and travel card numbers. • Release link trunk (RLT) allows an operator to bridge the calling and called parties on an operator-assisted call. • Multiple release link trunk (MRLT) allows the UCS DMS-250 switch to release multiple trunks connected to switches within the call path. ***Note:*** For more information on URLT0001 see the *UCS DMS-250 SS7 RLT Application Guide.*
URLT0002	0 SS7 RLT Enh Reorig	URLT0002 provides support for boomerang reorigination to a host EOPS UCS DMS-250 switch and an enhanced services platform (ESP). ***Note 1:*** You must have SOC URLT0001 to use SOC URLT0002. ***Note 2:*** For more information on URLT0002, see the *UCS DMS-250 SS7 RLT Application Guide.*

Table A-15 (Sheet 3 of 3)

Order Code	Name	Description
URLT0003	0 Nonzero SS7 RLT	URLT0003 provides RLT to non-zero-minus (0-) and non-zero-plus (0+) calls, which are non-operator calls routed to operator services on an RLT SS7. The RLT for non-operator calls uses the operator message builder rather than the standard SS7 message builder. ***Note 1:*** You must have SOC URLT0001 to use SOC URLT0003. ***Note 2:*** For more information on URLT0003, see the *UCS DMS-250 SS7 RLT Application Guide.*
URLT0004	0 SS7 RLT Billing En	URLT0004 allows the ESP, on a per-call basis: • to populate the BILLNUM, ACCTCD, PINDIGS, and UNIVACC fields in the CDR • to specify whether first or last ANM billing should be used for the call ***Note 1:*** You must have SOC URLT0001 to use SOC URLT0004. ***Note 2:*** For more information on URLT0004, see the *UCS DMS-250 SS7 RLT Application Guide.*

Translations and routing SOCs

Table Table A-16, “,” on page A-33, “Translations and routing SOCs," provides a comprehensive list of the translations and routing SOCs.

Table A-16 (Sheet 1 of 4)

Order Code	Name	Description
Translations and routing SOCs		
UTRS0001	UCS Trans & Rout	UTRS0001 provides specialized routing services on the UCS DMS-250 switch: • Carrier ID Code Routing uses Carrier Identification Code (CIC) digits to route incoming calls. • Network Operator Routing Enhancement routes operator calls across a UCS DMS-250 system network to a particular operator services provider, based on: — authorization code (authcode) — automatic number identification (ANI) — carrier identification code (CIC) — trunk group ***Note:*** For more information on UTRS0001, see the *UCS DMS-250 Feature Group D Application Guide.*
UTRS0002	Flexible Dial Plans	UTRS0002 allows operating companies to construct customized dialing plans on the UCS DMS-250 switch. ***Note:*** For more information on UTRS0002, see the *UCS DMS-250 FlexDial Framework Application Guide.*

Table A-16 (Sheet 2 of 4)

Order Code	Name	Description
UTRS0003	Routing Enh I	UTRS0003 provides three routing enhancements: • Answer CDR Generation allows operating companies to specify that they want a call detail record (CDR) to be generated when an Answer indication is received from the far end on a terminating route basis. Normally, a CDR record is generated when a call is completed. When the Answer CDR capability is enabled for a specified terminating route, CDR records are generated upon the call being answered as well as when the call is disconnected. • Cause Mapping Enhancements allow operating companies to specify for each-cause basis whether the UCS DMS-250 switch should advance to the next element in the routing list or whether it should retranslate the call. The option to retranslate the call is only available if the call originated on the new AXXESS trunk agency associated with the Flexible Dialing Plan feature. • Outgoing Parameter Modification allows operating companies to control the delivery of the following SS7 parameters on a terminating route basis: — Calling Party Number (CPN) — Charge Number (CGN) — Transit Network Selector (TNS) — Carrier Identification Parameter (CIP) — Generic Digits Parameter — Generic Address Parameter Operating companies can specify, through table datafill, which of these optional parameters they will include and exclude from the outgoing SS7 messages. Also, operating companies can specify whether the Dialed Number will replace the CPN number. ***Note:*** For more information on UTRS0003, see the *UCS DMS-250 international Application Guide*

Table A-16 (Sheet 3 of 4)

Order Code	Name	Description
UTRS0004	COS Screening Enh	UTRS0004 provides two enhancements to class of service (COS) screening: • COS Screening Treatment Granularity enhances the UCS DMS-250 switch's COS screening by: — providing a unique treatment for each reason a call can fail COS screening — allowing operating companies to specify for each reason a call can fail COS screening whether the call will route to a treatment, an announcement, or a tone • Time of Day (TOD) Restriction Table Expansion enhances TOD screening by: — increasing the maximum number of time of day restriction profiles from four to 255 — increasing the maximum number of time of day restriction time periods from five to eight for each profile ***Note:*** For more information on UTRS0004, see the *UCS DMS-250 International Application Guide*
UTRS0005	Ans Supv on UA	UTRS0005 provides an early answer indicator to the originator for universal access (UA) calls before sending tone and receiving address digits. Specifically, this feature sends an Answer Message (ANM) immediately after an Address Complete Message (ACM), in order for intermediate switches to cut-through voice path and to enable the collection of DTMF digits.

Table A-16 (Sheet 4 of 4)

Order Code	Name	Description
UTRS0200	Mult Prof ANI by CIC	UTRS0200 allows you to offer your subscribers, and other carriers' subscribers, unique feature sets based on the ANI and the CIC.
UTRS0201	Mult ANI Prof by Jur	UTRS0201 allows you to offer your subscribers, and other carriers' subscribers, unique feature sets based on the ANI, CIC, and jurisdiction for SS7 Feature Group D (FGD) originations. This SOC is used to control the jurisdiction call processing functionality of table MULTPROF. The SOC, UTRS0200 - Mult Prof ANI by CIC is required in order to use UTRS0201. If UTRS0201 is idle, tables ANIVAL MULTPROF, LATAID and LATASCRN may still be datafilled. However, access to table LATASCRN functionality during call processing is blocked

Appendix B SOC Logs

This appendix shows the format, an example, and the recommended action for each of the software optionality control (SOC) logs. For detailed descriptions of the logs, refer to the *UCS DMS-250 Logs Reference Manual*.

The SOC logs are divided into the following ranges:

- Range 300-399—critical or service-affecting issues within SOC or its applications that require user action for correction.
- Range 400-499—SOC audit reports.
- Range 500-599—SOC option and feature state changes.
- Range 600-799—non-critical or non-service-affecting issues within SOC or its applications that do not require any user action. These logs are strictly informational.
- Range 800-899—CAIN SOCs only.

CAIN102

When the switch attempts to access a CAIN feature, but the feature's SOC option has not been enabled, the switch creates CAIN102 log reports.

CAIN102 format

The format for log report CAIN102 follows:

CAIN102 mmdd hh:mm:ss nnnn INFO CAIN SOC ACCESS
Feature: <SOC feature identifier>
Option: <SOC option identifier>
Reason: <reason description>

CAIN102 example

The following is an example of log report CAIN102:

```
CAIN102 JUN24 18:14:33 0300 INFO CAIN SOC ACCESS
   FEATURE: BY801321
   OPTION:  CAIN0201
   REASON:  Feature SOC option is not ON
```

SOC300

The SOC periodic audit creates the SOC300 log. This log indicates a feature that was unexpectedly found in a troubled state. A troubled state is any state except IDLE or ON.

This log indicates either internal data inconsistencies or partial or incomplete SOC feature functionality.

The alarm level associated with this log is major.

SOC300 format

The format for log report SOC300 follows:

SOC300 mmdd hh:mm:ss nnnn TBL Audit
Feature: <SOC feature identifier>
State: <state name or numeric value>
Reason: <reason description>

SOC300 example

The following is an example of log report SOC300:

```
SOC300 SEP05 18:14:33 7815 TBL Audit
   FEATURE: AD883302
   OPTION:  CAIN0300
   REASON:  Feature was found to be in an invalid state
```

SOC300 action

Contact Nortel Emergency Technical Assistance Service (ETAS) for assistance.

Keep any software errors (SWERRs) or SOC logs related to this problem. Save all data to assist in problem identification and resolution.

SOC301

The SOC301 log is created during the SOC periodic audit. This log indicates an option that was unexpectedly found in a troubled state. A troubled state is any state except IDLE or ON.

This log indicates either internal data inconsistencies or partial or incomplete SOC option functionality.

The alarm level associated with this log is major.

SOC301 format

The format for log report SOC301 follows:

SOC301 mmdd hh:mm:ss nnnn TBL Audit
Option: <SOC feature identifier>
State: <state name or numeric value>
Reason: <reason description>

SOC301 example

The following is an example of log report SOC301:

```
SOC301 JUN12 14:49:27 8219 TBL Audit
    Option: CRDS0001
    State:  STATE ERROR
    Reason: Option was found to be in an invalid
            state
```

SOC301 action

Contact Nortel ETAS for assistance.

Keep any SWERRs or SOC logs related to this problem. Save all data to assist in problem identification and resolution.

SOC302

The SOC302 log is created when a problem with a feature is detected during an audit. This log is created for problems relating to internal data inconsistencies and to partial or incomplete functionality of a feature.

The alarm level associated with this log is minor.

SOC302 format

The format for log report SOC302 follows:

SOC302 mmmdd hh:mm:ss nnnn TBL Audit Failure
Feature: <SOC feature identifier>
Reason: <reason description>

SOC302 example

The following is an example of log report SOC302:

```
SOC302 JUN12 14:49:32 8623 TBL Audit failure
    Feature:CALLCARD
    Reason: failed to audit (trapped or timed out)
```

SOC302 action

Contact Nortel ETAS for assistance.

Keep any SWERRs or SOC logs related to this problem. Save all data to assist in problem identification and resolution.

SOC303

The SOC303 log is created during the SOC periodic audit. This log indicates an option has failed to be audited.

This log indicates either internal data inconsistencies or partial or incomplete SOC option functionality.

The alarm level associated with this log is minor.

SOC303 format

The format for log report SOC303 follows:

SOC303 mmdd hh:mm:ss nnnn TBL Audit failure
Option: <SOC option identifier>
Reason: failed to audit (data access error) ; results uncertain

SOC303 example

The following is an example of log report SOC303:

```
SOC303 JUN12 14:49:38 8926 TBL Audit failure
   Option:  CRDS0001
   Reason:  failed to audit (data access error);results
            uncertain
```

SOC303 action

Contact Nortel ETAS for assistance.

Keep any SWERRs or SOC logs related to this problem. Save all data to assist in problem identification and resolution.

SOC304

The SOC304 log is created during the SOC periodic audit. This log indicates that an option and a member feature are in different states.

This log indicates either internal data inconsistencies or partial or incomplete SOC option functionality.

The alarm level associated with this log is minor.

SOC304 format

The format for log report SOC304 follows:

SOC304 mmdd hh:mm:ss nnnn TBL Audit

	Identifier	State	Time
Option:	<option id>	<state value>	YY/MM/DD
Feature:	<feature id>	<state value>	YY/MM/DD
Reason:	Option and its feature state mismatch		

SOC304 example

The following is an example of log report SOC304:

```
SOC304 JUN12 14:49:38 9027 TBL Audit
            Identifier  State       Time
            ---------   -----       ----
   Option:  CRDS0001    ON          94/06/12
   Feature: CALLCARD    IDLE        94/06/12
   Reason:  Option and its feature state mismatch
            uncertain
```

SOC304 action

Contact Nortel ETAS for assistance.

Keep any SWERRs or SOC logs related to this problem. Save all data to assist in problem identification and resolution.

SOC305

The SOC305 log is created during the SOC periodic audit. This log indicates that a SOC and a feature are in different states.

This log indicates either internal data inconsistencies or partial or incomplete SOC option functionality.

The alarm level associated with this log is minor.

SOC305 format

The format for log report SOC305 follows:

SOC305 mmdd hh:mm:ss nnnn TBL Audit

Feature:	AN0408__	
	State	Troubled
	_____	_____
Feature:	<state value>	<trouble indicator>
SOC:	<state value>	<trouble indicator>
Reason:	SOC and feature data mismatch	

SOC305 example

The following is an example of log report SOC305:

```
SOC305 JUN12 14:49:38 9128 TBL Audit
   Feature: CALLCARD
            State               Troubled
            -----------         --------
   Feature: IDLE TO ON          YES
      SOC:  ON                  NO
   Reason:  SOC and feature data mismatch
```

SOC305 action

No action is required. SOC changes the option state to match the feature state.

SOC307

The SOC307 log is created during the SOC periodic audit. This log indicates that the SOC option database could not be accessed.

This log indicates either internal data inconsistencies or partial or incomplete SOC option functionality.

The alarm level associated with this log is major.

SOC307 format

The format for log report SOC306 follows:

SOC307 mmmdd hh:mm:ss nnnn TBL Audit

Feature:	<SOC feature identifier>
Option:	<SOC option identifier>
Reason:	<reason description>

SOC307 example

The following is an example of log report SOC307:

```
SOC307 JUN12 14:49:43 9431 TBL Audit
   Feature: CALLCARD
   Option:  CRDS0001
   Reason:  Feature is not in parent option's feature list
```

SOC307 action

Contact Nortel ETAS for assistance.

Keep any SWERRs or SOC logs related to this problem. Save all data to assist in problem identification and resolution.

SOC308

The SOC308 log is created any time the feature indicates to SOC that it is in a troubled state and SOC has not already recorded the trouble.

This log indicates partial or incomplete functionality.

The alarm level associated with this log is major.

SOC308 format

The format for log report SOC308 follows:

SOC308 mmmdd hh:mm:ss nnnn FAIL Feature troubled
Feature: <SOC feature identifier>
State: <state name or numeric value>
Reason: <reason description>

SOC308 example

The following is an example of log report SOC308:

```
SOC308 JUN12 14:49:43 9532 FAIL Feature troubled
   Feature: CALLCARD
   State:   IDLE
   Reason:  Feature is marked as troubled
```

SOC308 action

Contact Nortel ETAS for assistance.

SOC310

The SOC310 log is created when a problem with a SOC option is discovered during a SOC audit.

This log indicates either internal data inconsistencies or partial or incomplete SOC option functionality.

No alarm is associated with this log.

SOC310 format

The format for log report SOC310 follows:

SOC310 mmmdd hh:mm:ss nnnn TBL Audit
Option: <option>
Reason: <reason description>

SOC310 example

The following is an example of log report SOC310:

```
SOC310 JUN12 14:49:53 9633 TBL Audit
   Option:  CRDS0001
   Reason:  option is a member of its own precludes list
```

SOC310 action

If the reason is “state is ON but right to use not set," no immediate action is required. The option should eventually have its state set to IDLE or the RTU should be obtained and applied.

If the reason is other than “state is ON but right to use not set," keep a record of the log and contact next level of support.

SOC311

The SOC311 log is created when a feature fails to transition to the requested state at ONP time.

The alarm associated with this log is major.

SOC311 format

The format for log report SOC311 follows:

SOC311 mmmdd hh:mm:ss nnnn FAIL Software upgrade transition
Feature: <SOC feature identifier>
From: <state name or numeric value>
Request: <state name>
Result: <state name or numeric value>
Reason: <reason description>

SOC311 example

The following is an example of log report SOC311:

```
SOC311 JUN12 14:49:58 9936 FAIL Software upgrade transition
   Feature: CALLCARD
   From:    IDLE
   Request: ON
   Result:  IDLE
   Reason:  Cannot alloc memory
   Summary: Feature did not reach requested state
```

SOC311 action

Contact Nortel ETAS for assistance.

SOC312

The SOC312 log is created during the SOC periodic audit. This log indicates that a feature-related error was detected in the database.

The alarm associated with this log is minor.

SOC312 format

The format for log report SOC312 follows:

SOC312 mmmdd hh:mm:ss nnnn INFO Data mismatch
Option: <option>
Feature: <feature>
Reason: <reason description>

SOC312 example

The following is an example of log report SOC312:

```
SOC312 JUN12 14:49:58 0037 INFO Data mismatch
   Option:  CRDS0001
   Feature: CALLCARD
   Reason:  Feature belongs to a different option
```

SOC312 action

Contact Nortel ETAS for assistance.

SOC313

The SOC313 log is created during an audit or feature request if SOC detects one or more of the feature's SOC support procedures are invalid or unavailable.

The alarm associated with this log is major.

SOC313 format

The format for log report SOC313 follows:

SOC313 mmmdd hh:mm:ss nnnn TBL Audit
Feature: <SOC feature identifier>
The following procedures are invalid or unavailable:
<procedure list>

SOC313 example

The following is an example of log report SOC313:

```
SOC313 JUN12 14:49:58 0340 TBL Audit
   Feature: CALLCARD
   Reason:  The following procedures are invalid or
            unavailable:
            Audit, Impact, Reset, Software Upgrade,
            Transition, Validate
```

SOC313 action

Contact the personnel responsible for the next level of support. Keep any SWERRs or other SOC logs related to this problem to assist in problem identification and resolution.

SOC314

The SOC314 log is created when a problem related to a specific feature is discovered during a SOC audit.

The alarm associated with this log is major.

SOC314 format

The format for log report SOC314 follows:

SOC314 mmmdd hh:mm:ss nnnn TBL Audit
Feature: <feature>
Reason: <reason>

SOC314 example

The following is an example of log report SOC314:

```
SOC314 JUN12 14:50:03 0542 TBL Audit
   Feature: CALLCARD
   Reason:  Feature not a member of any option.
```

SOC314 action

Keep a record of the log and contact next level of support.

SOC315

The SOC315 log is created when a cycle has been found in the uses relationships between the named options. One of the two depends directly on the other, but the other also depends (either directly or through dependencies on other options) on the first option. This is an error, because it is impossible to know which option to turn on first.

A single instance of this log is never created. It is created for each option in the loop; examining all SOC315 logs (from a given audit) will indicate exactly what options are involved.

SOC315 format

The format for log report SOC315 follows:

SOC315 mmmdd hh:mm:ss nnnn TBL Audit
Option 1: <option_1>
Option 2: <option_2>
Reason: <reason>

SOC315 example

The following is an example of log report SOC315:

```
SOC315 AUG31 19:43:32 8200 TBL Audit
   Option 1: CRDS0001
   Option 2: CRDS0002
   Reason:   Options depend on each other (possibly
             indirectly)
```

SOC315 action

Keep a record of the log and contact the next level of support.

SOC316

The SOC316 log is created when a cycle has been found in the uses relationships between the named features. One of the two depends directly on the other, but the other also depends (either directly or through dependencies

on other features) on the first feature. This is an error because it is impossible to know which feature to turn on first.

A single instance of this log will never be created. It is created for each feature in the loop; examining all SOC316 logs (from a given audit) will indicate exactly what features are involved.

SOC316 format

The format for log report SOC316 follows:

SOC316 mmmdd hh:mm:ss nnnn TBL Audit
Feature 1: <feature_1>
Feature 2: <feature_2>
Reason: <reason>

SOC316 example

The following is an example of log report SOC316:

```
SOC316 AUG31 19:43:32 8300 TBL Audit
   Feature  1:  CALLCARD
   Feature  2:  TCAPCARD
   Reason:  Features depend on each other (possibly
            indirectly)
```

SOC316 action

Keep a record of the log and contact the next level of support.

SOC317

The SOC317 log is created when a SOC audit discovers the following situation: feature A in option X needs feature B in option Y, but feature B needs some other feature C in option X as well. The options cannot be turned on without violating dependency rules.

SOC317 format

The format for log report SOC317 follows:

SOC317 mmmdd hh:mm:ss nnnn TBL Audit
Feature 1: <feature_1> Option 1: <option_1>
Feature 2: <feature_2> Option 2: <option_2>
Reason: <reason>

SOC317 example

The following is an example of log report SOC317

```
SOC317 AUG31 19:43:32 8400 TBL Audit
   Feature  1:  AN0408__    Option 1: ENSV0007
   Feature  2:  AN0819__    Option 2: ABS00008
   Reason:  Implied loop in option depends due to feature
            depends
```

SOC317 action

Keep a record of the log and contact next level of support.

SOC318

The SOC318 log is created when an option depends on another option that is somehow illegal:

- the needed option is not defined
- the needed option precludes the named option
- the needed option is IDLE while the named option is ON

SOC318 format

The format for log report SOC318 follows:

SOC318 mmmdd hh:mm:ss nnnn TBL Audit
Option: <option>
Needed option: <needed_option>
Reason: <reason>

SOC318 example

The following is an example of log report SOC318:

```
SOC318 AUG31 19:43:32 8500 TBL Audit
   Option:  CRDS0002
   Needed option:   CRDS0001
   Reason:  Needed option is undefined (or pending)
```

SOC318 action

If the reason is “Needed option is in a less active state," either turn on the needed option or turn off the option that needs it.

If the reason is other than “Needed option is in a less active state," keep a record of the log and contact the next level of support.

SOC319

The SOC319 log is created when a feature depends on another feature that is somehow illegal:

- the needed feature is not defined
- the needed feature precludes the named feature

SOC319 format

The format for log report SOC319 follows:

SOC319 mmmdd hh:mm:ss nnnn TBL Audit
Feature: <feature>
Needed feature: <needed_feature>
Reason: <reason>

SOC319 example

The following is an example of log report SOC319:

```
SOC319 AUG31 19:43:32 8800 TBL Audit
   Feature: TCAPCARD
   Needed feature:  CALLCARD
   Reason:  Needed feature is undefined
```

SOC319 action

Keep a record of the log and contact next level of support.

SOC320

The SOC320 log is created for a problem in which feature A using feature B and precluding feature C, but features B and C are in the same option.

SOC320 format

The format for log report SOC320 follows:

```
)C320 mmmdd hh:mm:ss nnnn TBL Audit
 Feature:            <feature>           in Option:     <option>
 Needed Feature:     <need_feature>      in Option: <need_option>
 Precluded Feature:  <preclude_feature> in Option: <preclude_option>
 Reason: <reason>
```

SOC320 example

The following is an example of log report SOC320:

```
SOC320 AUG31    19:43:32    9000 TBL Audit
   Feature:         AN0408           in Option: ENSV0007
   Needed Feature:  AN0819   in Option:     ABS0008
   Precluded Feature:   AN0409   in Option:     ABS0008
   Reason:  Needed and precluded features are in same option
```

SOC320 action

Keep a record of the log and contact next level of support.

SOC321

The SOC321 log is created when a feature precludes another feature, but they are in the same option. The option cannot be turned on because the two mutually exclusive features would have to be on at the same time.

SOC321 format

The format for log report SOC321 follows:

SOC321 mmmdd hh:mm:ss nnnn TBL Audit
Feature: <feature> in Option: <option>
Precluded Feature: <precluded_feature>
Reason: <reason>

SOC321 example

The following is an example of log report SOC321:

```
SOC321 AUG31    19:43:32     TBL Audit
   Feature:         AN0408_         in Option: ENSV0007
   Precluded Feature:   AN0819_
   Reason:  Feature and precluded feature are in same option
```

SOC321 action

Keep a record of the log and contact the next level of support.

SOC322

The SOC322 log is created when a SOC audit finds both of two mutually exclusive options turned on.

SOC322 format

The format for log report SOC322 follows:

SOC322 mmmdd hh:mm:ss nnnn TBL Audit
Option: <option>
Precluded option: <precluded_option>
Reason: <reason>

SOC322 example

The following is an example of log report SOC322:

```
SOC322 AUG31    19:43:32    9200 TBL Audit
   Option:          ENSV0007
   Precluded option:    ABS00008
   Reason:  Option and precluded option are both ON
```

SOC322 action

One or both of the mutually exclusive options should be set to IDLE.

SOC323

This log is created when a SOC audit finds a usage-only option with dependencies on or preclusions with another option. Only state and combination options can have dependencies and preclusions.

SOC323 format

The format for log report SOC323 follows:

SOC323 mmmdd hh:mm:ss nnnn TBL Audit
Option: <option>
Needed option: <needed option>
Usage based option has dependencies

SOC323 example

The following is an example of log report SOC323:

```
SOC323  JUN12   14:50:03     0542  TBL Audit
   Option:  CAIN0400
   Needed option:  CAIN0100
   Reason:  Usage based option has dependencies
```

SOC323 action

This log indicates a serious error in the SOC database. Contact the personnel responsible for the next level of support.

SOC324

The SOC324 log is created when a SOC audit finds a usage-only feature with dependencies on or preclusions with another feature. Only state or combo features can have dependencies or preclusions.

SOC324 format

The format for log report SOC324 follows:

SOC324 mmmdd hh:mm:ss nnnn TBL Audit
Feature: <feature>
Usage based feature has dependencies

SOC324 example

The following is an example of log report SOC324:

```
SOC324  JUN12   14:50:03     0542  TBL Audit
   Feature: AD832802
   Reason:  Usage based feature has dependencies
```

SOC324 action

This log indicates a serious error in the SOC database. Contact the personnel responsible for the next level of support.

SOC325

The SOC325 log is created when a SOC audit finds an option with an illegal usage limit. A legal usage limit is from 0 to 999999.

SOC325 format

The format for log report SOC325 follows:

SOC325 mmmdd hh:mm:ss nnnn TBL Audit
Option: <option>
Limit: <limit>
Reason: <reason>

SOC325 example

The following is an example of log report SOC325:

```
SOC325  JUN12   14:50:03     0542  TBL Audit
   Option:  CAIN0400
   Limit:   –5
   Reason:  Limit must not be below zero
```

SOC325 action

Request a password for a correct usage limit from Nortel. Use the ASSIGN LIMIT command to apply the correct usage limit to the option.

SOC326

The SOC326 log is created if the features that make up an option do not match the type of the option. The following rules apply to features in options:

- A state option must contain at least one state-only feature, and no other type of feature.
- A usage option must contain one usage-only feature and no other features.
- A combination option must contain either one usage-only feature and one or more state-only features, or one combo feature and zero or more state-only features.

SOC326 format

The format for log report SOC326 follows:

SOC326 mmmdd hh:mm:ss nnnn TBL Audit
Option: <option>
Reason: <reason>

SOC326 example

The following is an example of log report SOC326:

```
SOC326  JUN12   14:50:03     0542  TBL Audit
   Option:  CAIN0401
   Reason:  Usage option contains state/combo feature
```

SOC326 action

This log indicates a serious error in the SOC database. Contact Nortel ETAS support.

SOC400

The SOC400 log is created at the end of a SOC audit. It summarizes the results of the audit and reports the total number of registered options in the IDLE state, in the ON state, in a trouble state and with the right-to-use (RTU) set. It also specifies the total number of errors that created logs during the audit.

Options in a trouble state may have incomplete functionality.

SOC400 format

The format for log report SOC400 follows:

SOC400 mmmdd hh:mm:ss nnnn SUMM SOC option audit summary

Total	IDLE	ON	TBL	RTU	ERRS
<nnnnn>	<nnnnn>	<nnnnn>	<nnnnn>	<nnnnn>	<nnnnn>

SOC400 example

The following is an example of log report SOC400:

```
SOC400 JUN12    14:50:03     SUMM SOC option audit summary
     Total    IDLE      ON      TBL         RTU     ERRS
    ------   ------   ------  ------      ------   ------
         6       4       2       1           2        1
```

SOC400 action

If the ERRS field is not zero, check the SOC logs to determine the errors and take appropriate action.

SOC402

This log is created during an audit in which SOC detects that the current usage of an option exceeds its warning threshold. This log tells the operating company that usage is nearing the limit for this option.

SOC402 format

The format for log report SOC402 follows:

SOC402 mmmdd hh:mm:ss nnnn INFO Usage Exceeds Threshold
Option: <option>
Usage: <usage>
Threshold:<threshold>
Limit: <limit>

SOC402 example

The following is an example of log report SOC402:

```
SOC402  JUN12   14:50:03 0542  INFO Usage Exceeds Threshold
   Option:  CAIN0400
   Usage:   255
   Threshold: 50%
   Limit:   500
```

SOC402 action

No action is required.

SOC403

This log is created during an audit in which SOC detects an option with a current usage that exceeds its limit. This log indicates an error only if the usage limit is hard.

SOC403 format

The format for log report SOC403 follows:

SOC403 mmmdd hh:mm:ss nnnn INFO Current Usage Exceeds Limit
Option: <option>
Usage: <usage>
Limit: <limit>

SOC403 example

The following is an example of log report SOC403:

```
SOC403  JUN12 14:50:03 0542 INFO Current Usage Exceeds Limit
   Option:  CAIN0400
   Usage:   506
   Limit:   500S
```

SOC403 action

If the limit of the option is hard (no suffix “S"), this log indicates an error condition. The operating company immediately must reduce usage of the resource controlled by this option or buy a higher limit from Nortel.

If the limit of this option is soft (with suffix “S"), no immediate action is required. The contract under which this option was purchased dictates the appropriate action.

SOC404

This log is created during an audit in which SOC detects that the usage of an option has exceeded 2147483647, which is as high as SOC can count. The limit for the option must be soft or monitored for this condition to exist. SOC

continues to allow allocation of resources, but does not allow decrementing of resources because it has no number from which to subtract.

SOC404 format

The format for log report SOC404 follows:

SOC404 mmmdd hh:mm:ss nnnn INFO SOC Usage Has Overflowed
Option: <option>
Usage: <usage>
Usage is greater than 2147483647

SOC404 example

The following is an example of log report SOC404:

```
SOC404  JUN12  14:50:03 0542  INFO SOC Usage Has Overflowed
   Option:  CAIN0400
   Usage:   506
   Usage is greater than 2147483647
```

SOC404 action

Contact the personnel responsible for your next level of support. The usage counter of the option should be reset.

SOC500

The SOC500 log is created when a feature successfully transitions to a stable state after having been in a troubled transition state.

SOC500 format

The format for log report SOC500 follows:

SOC500 mmmdd hh:mm:ss nnnn PASS State transition
Feature: <SOC feature identifier>
User: <user name> Terminal: <terminal name>
From: <state name or numeric value>
Result: <state name or numeric value>
Reason: <reason description>

SOC500 example

The following is an example of log report SOC500:

```
SOC500 JUN12 14:50:03 1047 PASS State transition
   Feature: CALLCARD
   User:    OPERATOR            Terminal:   TTY0
   From:    IDLE TO ON
   Result:  ON
   Reason:  Recovery to stable state from transition state
```

SOC500 action

No action is required.

SOC501

This log is created when an option has successfully changed state.

SOC501 format

The format for log report SOC501 follows:

SOC501 mmmdd hh:mm:ss nnnn PASS State Transition

Option:	<option>		
User:	<user>	Terminal:	<terminal>
From:	<from state>		
Result:	<result state>		
Reason:	<reason>		

SOC501 example

The following is an example of log report SOC501:

```
SOC501 JUN12 14:50:03 1249 PASS State transition
   Option:  CRDS0001
   User:    OPERATOR            Terminal:   TTYO
   From:    IDLE TO ON
   Result:  IDLE
   Reason:  NO IMPACT
```

SOC501 action

No action is required.

SOC502

This log is created when a feature fails to make the transition to the requested state.

SOC502 format

The format for log report SOC502 follows:

SOC502 mmmdd hh:mm:ss nnnn PASS State transition
Option: <option>
User: <user name> Terminal: <terminal name>
From: <state name or numeric value>
Target: <state name or numeric value>
Result: <state name or numeric value>
Reason: <reason description>

SOC502 example

The following is an example of log report SOC502:

```
SOC502 JUN12 14:50:08 1552 FAIL State transition
   Option:  CALLCARD
   User:    OPERATOR    Terminal:   TTY0
   From:    ON
   Target:  5 (unknown)
   Result:  ON
   Reason:  Invalid target state
```

SOC502 action

Keep a record of the log and contact the next level of support.

SOC503

The SOC503 log is created when an option failed to make the transition to a new state for one of a variety of reasons:

- the option's RTU was not set (IDLE=>ON only)
- one or more features failed to make the transition
- one or more features refused to make the transition

- changing state would create a dependency violation
- there are database inconsistencies that make it impossible to verify dependency safety

SOC503 format

The format for log report SOC503 follows:

SOC503 mmmdd hh:mm:ss nnnn FAIL State transition
Option: <option>
User: <user> Terminal:<terminal>
From: <from_state>
Target: <target_state>
Result: <result_state>
Reason: <reason>

SOC503 example

The following is an example of log report SOC503:

```
SOC503 JUN12 14:50:08 1552 FAIL State transition
   Option:  CRDS0001
   User:    OPERATOR    Terminal:   TTY0
   From:    ON
   Target:  IDLE
   Result:  ON
   Reason:  Right To Use not set
```

SOC503 action

Keep a record of the log and contact the next level of support.

SOC504

This log is created when an option has been granted the RTU.

SOC504 format

The format for log report SOC504 follows:

SOC504 mmmdd hh:mm:ss nnnn INFO RTU is set
Option: <option>
User: <user> Terminal: <terminal>
Reason: <reason>

SOC504 example

The following is an example of log report SOC504:

```
SOC504 JUN12 14:50:13 3062 INFO RTU is set
   Option:  CRDS0001
   User:    OPERATOR    Terminal:   TTYO
   Reason:  User request
```

SOC504 action

No action is required.

SOC505

This log reports the failure of an attempt to apply a SOC key code, to assign a usage limit, to apply an RTU, or to remove an RTU. This log specifies the current value, the reason for failure, and any SOC comments.

SOC505 format

The format for log report SOC505 follows:

SOC505 mmmdd hh:mm:ss nnnn INFO RTU is not set
Option: <option>
User: <user> Terminal: <terminal>
Reason: <reason description>

SOC505 example

The following is an example of log report SOC505:

```
SOC505 JUN12 14:50:13 3769 INFO RTU is not set
   Option:  CRDS0001
   User:    OPERATOR    Terminal:   TTYO
   Reason:  User request
```

SOC505 action

Keep a record of the log and contact the next level of support.

SOC506

This log is created when a feature has changed state, but SOC has not requested the feature to change its state.

SOC506 format

The format for log report SOC506 follows:

SOC506 example

The following is an example of log report SOC506:

```
SOC506 JUN12 14:50:19 4173 TRAN State transition
   Feature: CALLCARD
     From:  IDLE TO ON
   Result:  ON
   Reason:  Manual test
```

SOC506 action

Keep a record of the log and contact the next level of support.

SOC507

This log records the fact that the user changed the warning threshold for an option. When the current usage of an option exceeds the threshold, a SOC800 log is created; if the usage exceeds the threshold when an audit is run, a SOC402 log is created.

SOC507 format

The format for log report SOC507 follows:

SOC507 mmmdd hh:mm:ss nnnn INFO Option Threshold Change
Option: <option>
User: <user> Terminal: <terminal>
Old Threshold: <old threshold>
New Threshold: <new threshold>
Note: <note>

SOC507 example

The following is an example of log report SOC507:

```
SOC507  JUN12 14:50:19 4173  INFO Option Threshold Change
   Option: CAIN0401
   User: OPERATOR               Terminal: TTYO
   Old Threshold:   100%
   New Threshold:   75%
   Note: None
```

SOC507 action

No action is required.

SOC508

This log indicates that an attempt to set the warning threshold for an option failed. When the current usage of an option exceeds the threshold, a SOC800 log is created; if the usage exceeds the threshold when an audit is run, a SOC402 log is created.

SOC508 format

The format for log report SOC508 follows:

SOC508 mmmdd hh:mm:ss nnnn INFO Threshold Change Failed
Option: <option>
User: <user> Terminal: <Terminal>
Current Threshold: <current threshold>
Reason: <reason>

SOC508 example

The following is an example of log report SOC508:

```
SOC508  JUN12 14:50:19 4173  INFO Threshold Change Failed
   Option: CAIN0401
   User: OPERATOR           Terminal: <Terminal>
   Current Threshold: 100%
   Reason: Requested threshold is illegal
```

SOC508 action

Take the appropriate action to address the problem in the Reason field and try to set the warning threshold again. An option with a monitored limit is only allowed a percentage threshold of 100 percent. This restriction may be the source of the error.

SOC509

The SOC509 log is created when the state of an option changes during a one-night process (ONP) because data transferred during the ONP specifies that the option should be ON after the ONP.

SOC509 format

The format for log report SOC509 follows:

SOC509 mmmdd hh:mm:ss nnnn INFO Feature Set Option's State
Option: <option> Feature: <feature>
From state: <from state> To state: <to state>
Number of required options also changed: <num changed>

SOC509 example

The following is an example of log report SOC509:

```
SOC509  JUN12 14:50:19 4173  INFO Feature Set Option's State
   Option: CAIN0100             Feature: AD832804
   From state: IDLE             To state: ON
   Number of required options also changed: 6
```

SOC509 action

No action is required.

SOC510

This log is created if an option tries to change its state during an ONP but fails. This is potentially a serious situation, since functionality that was in use before the ONP may not be enabled now.

SOC510 format

The format for log report SOC510 follows:

SOC510 mmmdd hh:mm:ss nnnn INFO ONP State Change Failed
Option: <option> Feature: <feature>
From state: <from state> Target state: <target state>
Reason: <reason>

SOC510 example

The following is an example of log report SOC510:

```
SOC510  JUN12 14:50:19 4173  INFO ONP State Change Failed
   Option: CAIN0100         Feature: AD83804
   From state: IDLE          Target state: ON
   Reason: Request option failed transition
```

SOC510 action

Take appropriate action to respond to the error in the Reason field.

SOC511

The SOC511 log is created for each option that changes state because the option requested a state change to conform to its state before the ONP.

SOC511 format

The format for log report SOC511 follows:

SOC511 mmmdd hh:mm:ss nnnn INFO ONP State Transition
Option: <option>
From state: <from state> To state: <to state>
Requesting Option: <option>
Reason: <reason>

SOC511 example

The following is an example of log report SOC511:

```
SOC511  JUN12 14:50:19 4173  INFO ONP State Transition
   Option: CAIN0100
   From state: IDLE         To state: ON
   Requesting Option: CAIN0300
   Reason: Needed by other option during data move
```

SOC511 action

No action is required.

SOC600

The SOC600 log is created during the ONP when the SOC database is transferred from the old side to the new side, if a feature on the old side is not transferred to the new side.

SOC600 format

The format for log report SOC600 follows:

SOC600 mmmdd hh:mm:ss nnnn INFO ONP feature data mismatch
Feature: <feature>
Reason: <reason>
State: <state> Last changed: <yy/mm/dd>

SOC600 example

The following is an example of log report SOC600:

```
SOC600 JUN12 14:50:19 4274 INFO ONP feature data mismatch
   Feature: CALLCARD
   Reason: Feature does not exist in new PCL, data has been
           discarded
   State: ON            Last changed: 92/02/29 12:35:17
```

SOC600 action

Determine if this information has been identified in the ONP procedural bulletins. If it has, no action is required. If it has not, contact Nortel for assistance.

SOC601

The SOC601 log is created during an ONP when the SOC database is transferred from the old side (before the ONP) to the new side (after the ONP). This log indicates that an old side option has not been registered with SOC on the new side and that the old side data has been discarded.

SOC601 format

The format for log report SOC601 follows:

SOC601 mmmdd hh:mm:ss nnnn INFO ONP option data mismatch
Option: <option>
Reason: <reason>
State: <state> Last changed: <yy/mm/dd>

SOC601 example

The following is an example of log report SOC601:

```
SOC601 JUN12 14:50:19 4375 INFO ONP option data mismatch
   Option:  CRDS0001
   Reason:  Option does not exist in new PCL, data has been
            discarded
   State:   ON          Last changed: 92/02/29 12:35:17
```

SOC601 action

Determine if this information has been identified in the ONP procedural bulletins. If it has, no action is required. If it has not, contact Nortel for assistance.

SOC602

This log is created during initial program load (IPL) to indicate that a feature has already registered with SOC, and that its previous data will be overwritten.

SOC602 format

The format for log report SOC602 follows:

SOC602 mmmdd hh:mm:ss nnnn INFO SOC bind overwrite
SOC bind of feature: <feature> overwrites previous binding

SOC602 example

The following is an example of log report SOC602:

```
SOC602 JUN12 14:50:19 4476 INFO SOC bind overwrite
   SOC bind of feature: CALLCARD overwrites previous binding
```

SOC602 action

No action is required.

SOC604

This log indicates that the SOC database has been reset to match the values of the feature.

SOC604 format

The format for log report SOC604 follows:

SOC604 mmmdd hh:mm:ss nnnn INFO SOC reset by feature
Feature: <feature>
State: <state>
Trouble: <YES or NO>

SOC604 example

The following is an example of log report SOC604:

```
SOC604 JUN12 14:50:24 4577 INFO SOC reset by feature
   Feature: CALLCARD
   State:   ON
   Trouble: NO
```

SOC604 action

No action is required.

SOC605

This log is created if there is a discrepancy between SOC's determination of an option's level of resource usage and the determination of the option itself. SOC assumes that the option is correct and updates its database.

SOC605 format

The format for log report SOC605 follows:

SOC605 mmmdd hh:mm:ss nnnn INFO Current Usage Mismatch
Option: <option>
Recorded Usage: <recorded usage>
Actual Usage: <actual usage>
SOC record has been updated to reflect actual usage

SOC605 example

The following is an example of log report SOC605:

```
SOC605  JUN12  14:50:24  4577 INFO Current Usage Mismatch
   Option: CAIN0401
   Recorded Usage: 500
   Actual Usage: 501
   SOC record has been updated to reflect actual usage
```

SOC605 action

This log indicates either that the SOC database has become corrupted or that the option has allocated or freed resources without a record. Contact the personnel responsible for your next level of support.

SOC606

This log indicates that SOC discovered an illegal usage warning threshold during an audit and therefore reset the warning threshold to the default.

SOC606 format

The format for log report SOC606 follows:

SOC606 mmmdd hh:mm:ss nnnn INFO Illegal Threshold
Option: <option>
Old Threshold: <old threshold>
New Threshold: <new threshold>
Threshold reset by SOC
Reason: <reason>

SOC606 example

The following is an example of log report SOC606:

```
SOC606  INFO Illegal Threshold
   Option: CAIN0401
   Old Threshold: 200%
   New Threshold: 75%
   Threshold reset by SOC
   Reason: Percentage threshold must be <= 100
```

SOC606 action

No immediate action is necessary. SOC has corrected the limit to a legal value. If another value is preferred, you can reset the warning threshold with the ASSIGN THRESHOLD command.

SOC607

The SOC607 log is created when the RESET HIGHWATER command is run by Nortel.

SOC607 format

The format for log report SOC607 follows:

SOC607 mmmdd hh:mm:ss ssdd INFO High Water Mark Reset
Option: <option>
Old High Water Mark: <old HWM>
New High Water Mark: <new HWM>

SOC607 example

The following is an example of log report SOC607:

```
SOC607 mmmdd hh:mm:ss ssdd INFO High Water Mark Reset
   Option: CAIN0401
   Old High Water Mark: 1234
   New High Water Mark: 5678
```

SOC607 action

No action is required.

SOC800

The SOC800 log is created when the current usage of an option increases to more than the warning threshold. For example, if the current usage was 495, the threshold was 500, and 10 more units were allocated, this log is created.

SOC800 format

The format for log report SOC800 follows:

SOC800 mmmdd hh:mm:ss nnnn INFO Usage Has Exceeded Threshold
Option: <option>
Usage: <usage>
Threshold:<threshold>
Limit: <limit>

SOC800 example

The following is an example of log report SOC800:

```
SOC800  INFO Usage Has Exceeded Threshold
   Option: CAIN0401
   Usage: 5001
   Threshold: 5000
   Limit: 6000
```

SOC800 action

No immediate action is required. However, this log indicates that the resource usage of this option is nearing its limit.

SOC801

This log is created when the usage limit of an option has been exceeded. This can occur either when the usage limit is soft or when the limit is exceeded during a data move. During a data move, SOC allows an option to exceed a hard limit to avoid loss of service.

SOC801 format

The format for log report SOC801 follows:

SOC801 mmmdd hh:mm:ss nnn INFO Usage Has Exceeded Limit
Option: <option>
Usage: <usage> Limit: <limit>
Comment: <comment>

SOC801 example

The following is an example of log report SOC801:

```
SOC801 JAN10 10:29:49 6415 INFO Usage Has Exceeded Limit
   Option:  SOCOPT04
   Usage:   10043           Limit:  10000S
   Comment: Exceeding SOFT limit
```

SOC801 action

No immediate action is required. However, if the reason was “Exceeding HARD limit on INACTIVE processor," the option is not permitted to have as many resources allocated as it has. Either reduce usage or contact Nortel to purchase a higher limit.

SOC802

This log is produced when the usage of an option exceeds 2147483647 which is as high as SOC can count. SOC continues to allow allocation of resources, but does not allow decrementing of resources, because it has no number from which to subtract.

SOC802 format

The format for log report SOC802 follows:

SOC802 mmmdd hh:mm:ss nnnn INFO Usage Has Overflowed
Option: <option>
Usage: over<max usage>
Comment: <comment>

SOC802 example

The following is an example of log report SOC802:

```
SOC802 JUN12 14:50:24 INFO Usage Has Overflowed
   Option:  CAIN0401
   Usage:   2147483647
   Comment: Further usage is allowed but will not be
            recorded
```

SOC802 action

No action is required.

SOC803

This log is created when an option tries to allocate more of a resource, but is refused by SOC because it would exceed the option's limit.

SOC803 format

The format for log report SOC803 follows:

SOC803 mmmdd hh:mm:ss nnnn INFO Usage Request Refused
Option: <option>
Current Usage: <usage>
Request: <request>
Limit: <limit>
Granting this request would cause usage to exceed the limit

SOC803 example

The following is an example of log report SOC803:

```
SOC803 JUN12 14:50:24 4577 INFO Usage Request Refused
   Option:  CAIN0401
   Current Usage: 4995
   Request: 10
   Limit:   5000
   Granting this request would cause usage to exceed the
   limit
```

SOC803 action

No immediate action is required. However, this log identifies a potentially serious situation. It indicates that the office cannot utilize more of the specified resource or count more of the specified event. For example, if the event is AIN triggers, AIN functionality may be reduced until the limit is increased.

Appendix C List of terms

ASSIGN command

The ASSIGN command allows you to enable the right-to-use for an option, assign a usage limit to an option, change the state of an option, or assign a warning threshold to an option.

brief report

The brief report contains one line of information for each option in the operating company's software load.

CI

Command interface

dual option

A dual option is usage-controlled and can also be set to on or idle.

DBAUDIT command

The DBAUDIT command allows you to tell the system to perform an audit of the SOC database. SOC does regular audits automatically. The audit requested by the DBAUDIT command provides the user with the information at the MAP terminal, in addition to the logs created by the audit.

deactivation

When an option is deactivated, it is turned to the idle state. Before SOC deactivates an option, it displays messages that describe the impact of the deactivation and it asks you to confirm or cancel the state change.

IDLE state

An option in the idle state is not operational.

idle-to-on state

Idle-to-on is a transitional state. If an error occurs during the state transition and the option can neither revert to the idle state nor change to the on state, the option is in the idle-to-on state.

ITO

See idle-to-on state.

high water mark

The high water mark is the option's highest level since either it was created or since its high water mark was reset.

key code

A key code is an alphanumeric password that Nortel gives to the operating company for every option that a customer is entitled to use. Every operation for every option in a DMS office requires a unique key code.

NORTEL_ID

The NORTEL_ID is the unique identifier Nortel assigns to every DMS office.

ON state

An option in the ON state is fully operational.

on-to-idle state

On-to-idle is a transitional state. If an error occurs during the state transition and the option can neither revert to the on state nor change to the idle state, the option is in the on-to-idle state.

option

An option is any optional capability that an operating company can purchase in a PCL.

order code

An order code is the alphanumeric identifier Nortel assigns to an option.

OTI

See on-to-idle state.

pack report

The pack report is a compressed version of the brief report for all options. It is used to provide status about options to Nortel.

PADNDEV

Patch administration and downloading device (PADNDEV) is a table that specifies a list of devices for reading and writing files.

PCL

See product computing module load.

pending option

A pending option is a placeholder for an option that will be downloaded at a later date.

product computing module load

A product computing module load is the computing module software load delivered to the customer.

right-to-use

Right-to-use (RTU) for an option must be granted to the operating company in order for the operating company to change the state of the option. Changing the state of the option requires a password supplied by Nortel.

RTU

See right-to-use.

SELECT command

The SELECT command enables the user to display information about SOC options or to create a report about SOC options.

SOC

See software optionality control.

SOC option

Optional capabilities are grouped into commercial units called SOC options. A SOC option can be ordered by the operating company. It is managed by the SOC utility.

software application

A software application is the process by which new software is loaded into the switch.

software optionality control

Software optionality control (SOC) is the utility that provides the operating company the capability to enable or disable SOC options. SOC is part of the DMS Evolution product delivery process.

state option

A state option is in on or idle state; the RTU for the option is set to yes or no.

tracked option

A tracked option is not controlled by SOC, but it is tracked by the SOC database. SOC can create a complete record of the purchase status of all options in an operating company's load.

usage limits

A usage limit can be hard, soft, or monitored. A hard usage limit cannot be exceeded, whereas a soft usage limit can be exceeded. A log is created when a hard or soft limit is reached. Monitored usage specifies the usage of the option is recorded but not limited by SOC.

usage option

SOC tracks and controls the use of a usage option. A usage option has a limit (hard, soft or monitored) and a current usage. The usage limit of the option determines the RTU:

- if the limit is zero, the RTU is no
- if the limit is greater than zero
- the RTU is yes

verbose report

The verbose report contains several lines of information for each option in the operating company's software load.

warning threshold

The warning threshold of an option is the level of usage at which SOC creates a log to inform the operating company that the usage of a resource is nearing its limit. The warning threshold can be set at a percentage of the usage limit or to an absolute number. It is assigned to the option by the operating company.

Digital Switching Systems

UCS DMS-250

Software Optionality Control User's Manual

Publication number: 297-2621-301
Product release: UCS17
Document release: Standard 10.03
Date: July 2002
Printed in the United States of America

NORTEL NETWORKS™